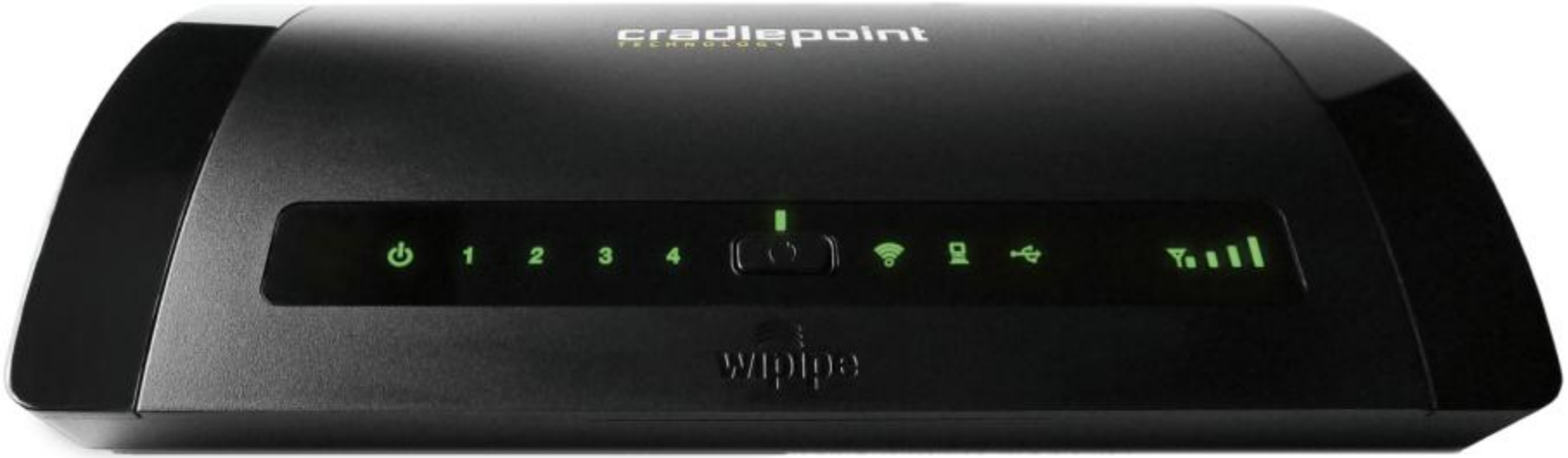
MBR95

PRODUCT MANUAL

Wireless 4G/3G Router



wipipe POWERED

bg WiFi n CERTIFIED

for additional information, visit:

knowlegebase.cradlepoint.com

Preface

CradlePoint reserves the right to revise this publication and to make changes in the content thereof without obligation to notify any person or organization of any revisions or changes.

Manual Revisions

Revision	Date	Description	Author
1.0	July 19, 2011	Initial release for Firmware version 3.2.4	Jeremy Cramer

Trademarks

Table of Contents

1 INTRODUCTION

1.1 *Package Contents*

- Wireless 4G/3G Router (MBR95)
- AC power adapter (12V, 1.5A) WARNING: using a power adapter other than the one provided may damage the MBR95 and will void the warranty
- CAT5 Ethernet Cable (5 feet)
- Setup Guide

1.2 *System Requirements*

- Ethernet-based, Cable/DSL/Satellite modem; Broadband USB Data Modem with Active Subscription; and/or WiFi as WAN.
- Windows 2000/XP/7, Mac OS X, or Linux Computer with WiFi Adapter (802.11n Recommended)
- Internet Explorer v6.0 or higher, Firefox v2.0 or higher, Safari v1.0 or higher.

1.3 *MBR95 Overview*

Create a WiFi hotspot anywhere you have broadband signal
Create secure instant networks anywhere you receive mobile broadband signal. The most powerful feature of the MBR95 is its ability to use USB Mobile Broadband Data Modems to create instant secure networks, plus traditional wired networking options like Cable, DSL, or Satellite.

HOW DOES IT WORK?
Connect this router to a 4G/3G MOBILE MODEM and get more from your data plan. Most WiFi enabled devices don‘t support USB 4G/3G Data Modems. When you connect the modem to the MBR95, you can securely share your data plan with up to 32 people or devices.

Or, connect this router to your existing DSL / CABLE / SATELLITE MODEM and add 600 feet of WiFi to your network.

CradlePoint routers are built to work with most popular 4G/3G USB Modems from: AT&T, Bell Canada, Clearwire, Cricket, Rogers, Sprint, T-Mobile, Telus, US Cellular, Verizon Wireless, & Virgin Mobile, as well as most Cable, DSL, and Satellite providers.

ENHANCED WIFI

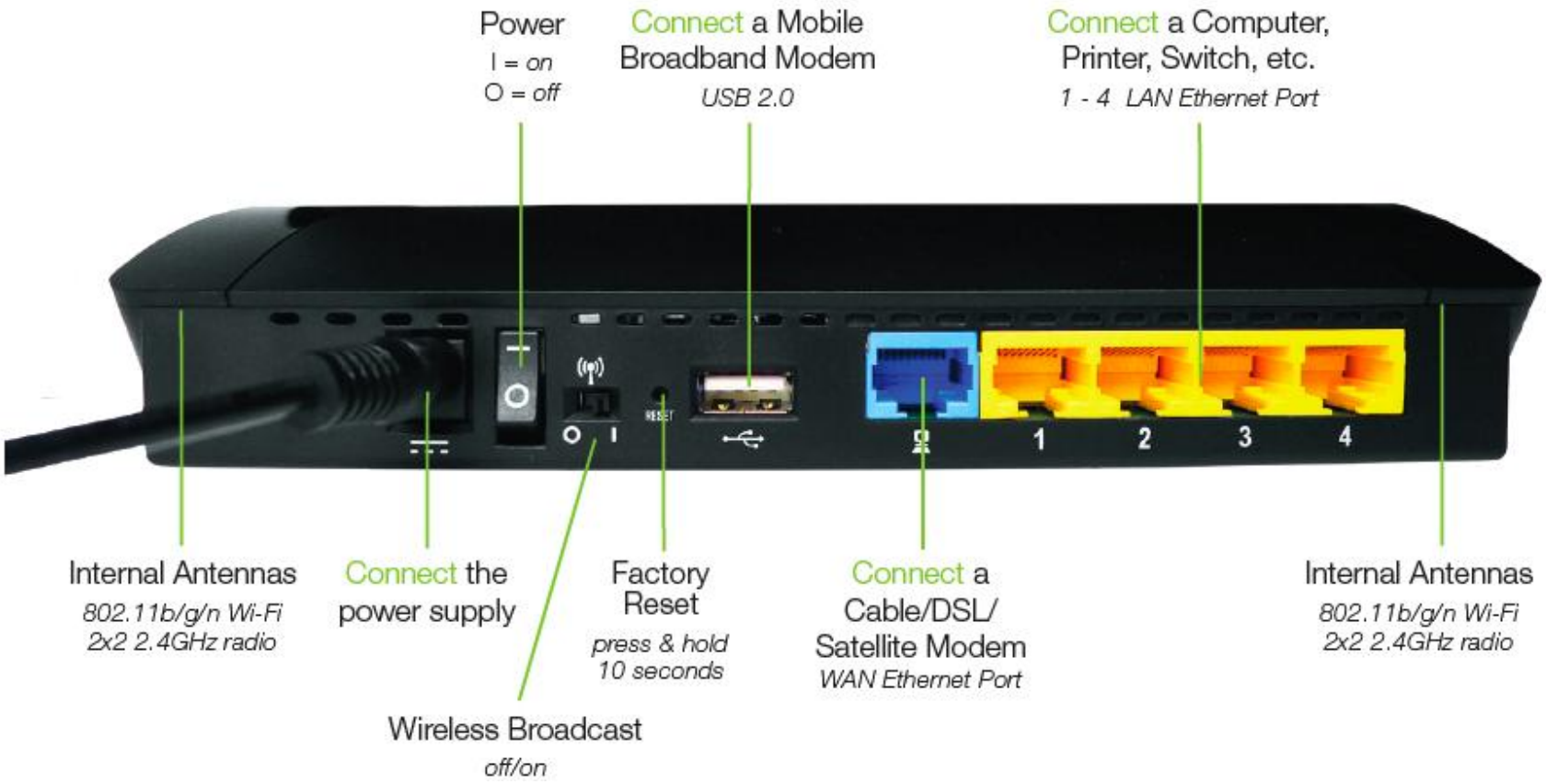
- 600+ feet of WiFi Range
- Wireless —NWiFi (802.11n, legacy 802.11b/g, 2x2 MIMO Internal Antenna system)
- Enhanced performance around walls and other obstructions
- Maximum security with both Private and Guest networks

ADDITIONAL FEATURES

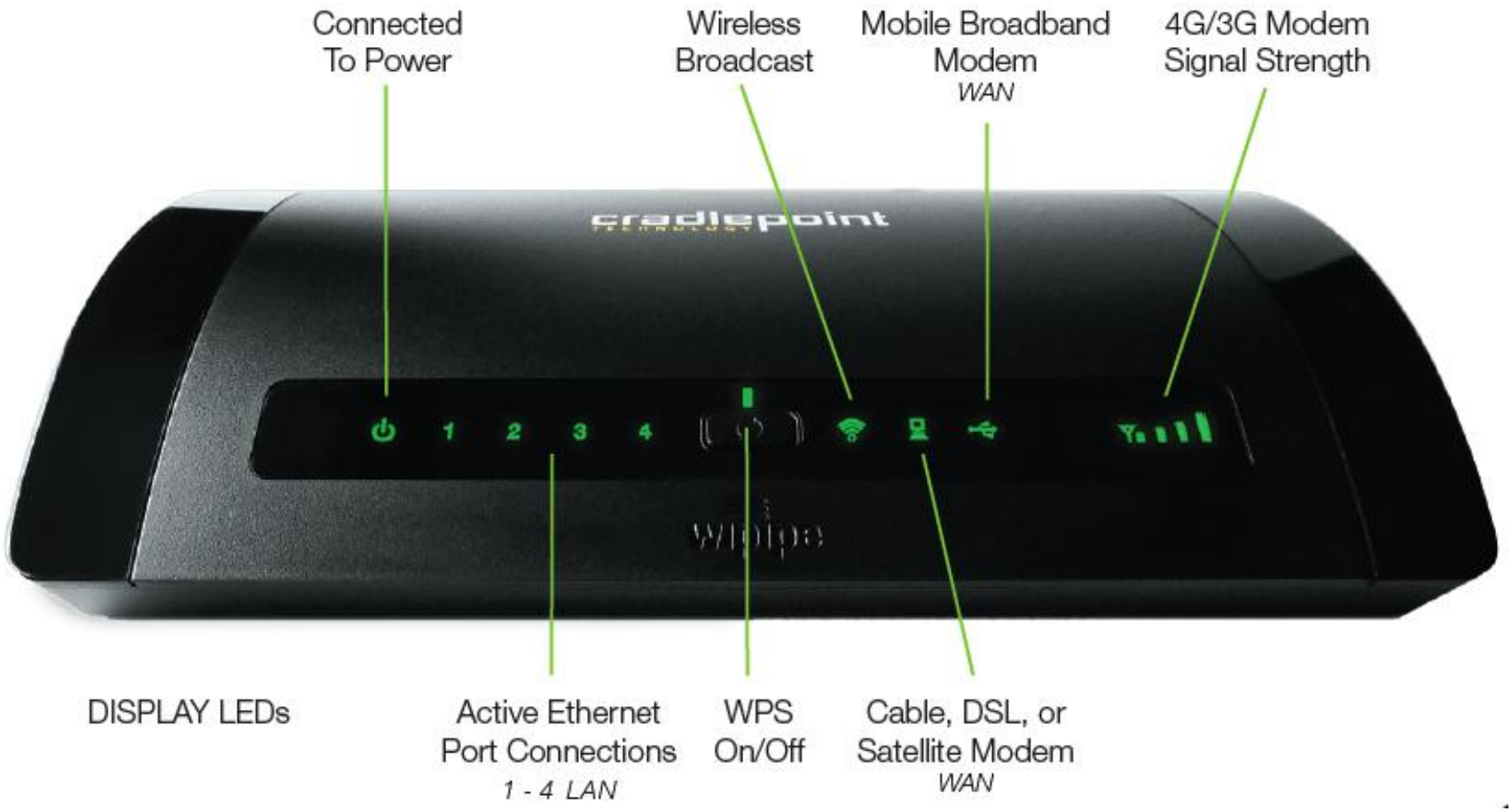
- 2x2 MIMO Internal Antenna Subsystem, dual SSIDs
- Plug-and-Play support for over 120 broadband data modems including LTE, WiMAX and HSPA+, allowing for maximum flexibility
- Simple to install, configure and maintain

2 HARDWARE OVERVIEW

2.1 *Ports, Buttons, and Switches*



2.2 *LEDs*



Power: The MBR95 must be powered using an approved 12V DC power source.

- Green = Powered on.
- No Light = Not receiving power. Check that the unit is connected to an outlet.
- Amber = Attention. Check router status page.

Active Ethernet Port Connections – *1-4 LAN*: Indicates a connected device on the 1-4 LAN ports on the MBR95.

- Blue = Connected to an active 10/100 Ethernet interface.
- Blinking Blue = Traffic.
- No Light = Not connected, the connection is not configured correctly, the router is not configured correctly, or the router may not be turned on.

WPS: WiFi Protected Setup. When you press the WPS button for five seconds, it allows you to use WPS for your WiFi security.

- Blinking Blue = WPS setting is in progress.
- Solid Blue = WPS is active.

Wireless Broadcast: Indicates activity on the WiFi broadcast for the 2.4 GHz band.

- Blue = 2.4 GHz WiFi is on and operating normally.
- Red = Error with 2.4 GHz connection.
- No Light = WiFi is off.

Cable, DSL, or Satellite Modem – *WAN*: Indicates information about a data source connected to the WAN Ethernet port (blue port).

- Blue = Connected to an active 10/100 Ethernet interface.
- Blinking Blue = Traffic.
- No Light = Not connected, the connection is not configured correctly, or the switch or router are not configured correctly or turned on.

Mobile Broadband Modem (USB) – *WAN*: Indicates the status of a USB modem connected to the MBR95.

- Blue = Modem has established an active 4G connection.
- Blinking Blue: Modem is connecting to 4G.
- Green = Modem has established an active 3G connection.
- Blinking Green = Modem is connecting to 3G.
- Amber = Modem is not active.
- Blinking Amber = Data connection error. No modem connection possible.
- Blinking Red = Modem is in the process of resetting.

4G/3G Modem Signal Strength: Blue LED bars indicate the active modem‘s signal strength. Press WPS button to turn on/off.

- 4 Solid Bars = strongest signal
- 1 Blinking Bar = weakest signal

3 QUICK START

3.1 *Basic Setup*

1) Connect the Router to a Modem or Data Source: Your router requires an internet source. Insert a supported USB modem; connect a Cable, DSL, or Satellite modem to the Blue Ethernet WAN port; or connect to an available WiFi source.

For Failover/Failback functionality, you will need at least two of these sources (for example: an Ethernet source and a USB modem).[1]

2) Connect to a Power Source: Connect the 12v DC power adapter to the router and a power source. Flip the power switch to the ON position; this should illuminate the green Power Status LED.

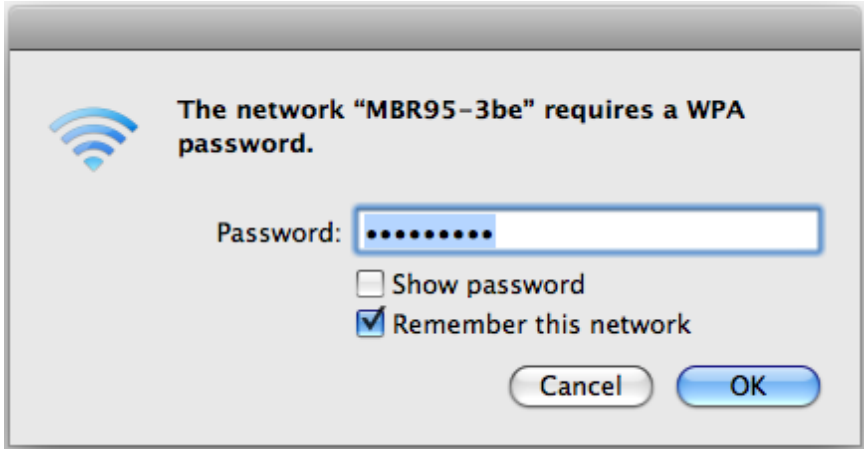
[1] Data Modem Not Included. This Product Requires an Activated Data Modem or Phone with Data Plan for Full Functionality. See your Cellular/3G/4G Service Provider for Details on Coverage and Data Plan Options

3.2 *Connect to a Computer or other Device*

3.2.1 Wireless Network Connection

1) Find the network. On a WiFi-enabled computer or device, open the window or dropdown menu that allows you to access wireless networks. The MBR95 network will appear on the list: select this network.

2) Log in. You will need to input the **Default Password** when prompted. The Default Password is provided on the product label found on the bottom of your router (this password is the last eight digits of the router's MAC address, which can be found on the product box or on the product label).



NOTE: If more than one MBR95 wireless router is visible, you can find the correct unit by checking for its **SSID** (service set identifier; the unique name of the local network). The SSID can be found on the bottom of the router in the form MBR95-xxx, where "xxx" is the last 3 digits of the router's MAC address.

3.2.2 Accessing the Administration Pages

For most users, the MBR95 Router can be used immediately without any special configuration changes. If you would like to change your network name or password or configure any of the advanced features of the MBR95, you will need to log in to the administration pages:

- Access your router's **Administrator Login** screen by opening a web browser window and typing "cp/" (your router's default hostname) or the IP address "192.168.0.1" into the address bar.
- Enter your **Default Password**. This password can be found on the bottom of the MBR95. Then click the **LOGIN** button.
- When you log in for the first time, you will be automatically directed to the **First Time Setup Wizard**. Follow the instructions given with the Wizard or see Getting Started – First Time Setup for more information about using the **First Time Setup Wizard**.

3.2.3 Connect to the Internet

If you used the **First Time Setup Wizard**, you might have changed the "WiFi Network Name" or the "Security Mode" password. If so, you will need to reconnect to the MBR95 network.

- **Find the network**. Look for your new personalized network name (or the default SSID of the form "MBR95-xxx").
- **Log in** using your new personalized WiFi security password (or the Default Password found the bottom of the router).

Your network should now be up and running, and users who have the security password can access the network on WiFi-enabled devices.

3.3 *Common Problems*

This section contains a list of some of the most common issues faced by users of the MBR95.

Please visit CradlePoint Knowledgebase at http://knowledgebase.cradlepoint.com/ for more help and answers to your other questions.

3.3.1 Your USB Modem Does Not Work With the Router

- If your USB data modem is not working with the router, check the list of supported devices at http://www.cradlepoint.com/modems to ensure you are using a supported device and carrier. The device you are using must be supported on the carrier network providing your cellular service or it's considered an unsupported device, even if it is supported on another carrier's network.

- Sometimes a USB data modem needs to be updated or have other configurations set correctly in order to make a connection through the router. If your USB Modem has not been updated recently, it is recommended that you do so if it is having trouble connecting to the MBR95. Insert your USB data modem into your PC and access the internet using the software provided by your cellular carrier. Follow the directions provided to complete the update. Once you have updated your USB data modem, reconnect the cellular device to your CradlePoint router and connect to the internet.

- If you are using a 4G WiMAX modem you need to set the WiMAX Realm. This can be done on the administration pages. Log in using the hostname "cp/" or IP address "http://192.168.0.1" in your browser. On page 3 of the First Time Setup Wizard (go to **Getting Started → First Time Setup**), you can set the WiMAX Realm. Be sure to click **Apply** on page 4 to save the change.

- Some wireless carriers provide more than one Access Point Name (APN) that a modem can connect to. If you wish to specify the APN, this can be done on the administration pages. Log in using the hostname "cp/" or IP address "http://192.168.0.1" in your browser. Go to **Internet → Modem Settings**. In the **Modem Configuration** section, select your modem and click "Configure." There is an Access Point Name field: Enter the APN and click **Apply**. Some APN examples are **isp.cingular**, **ecp.tmobile.com**, and **vpn.com**. The modem must be removed and reinserted (or the router must be rebooted) for this change to take effect.

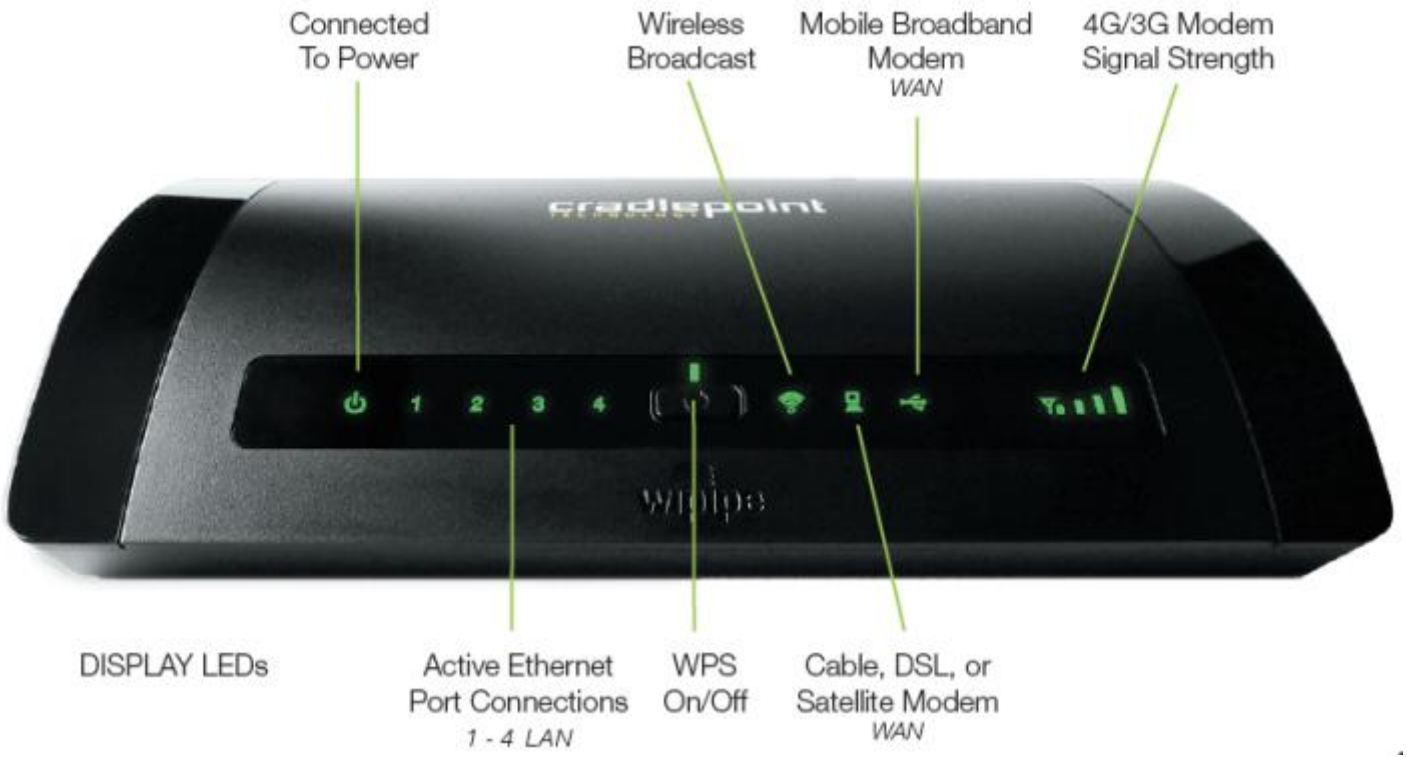
- If the above issues have been resolved and you can connect to the router but you cannot get internet through it using your modem, you may need to upgrade the router firmware. Use your computer (you may need to plug your modem directly into your computer if you don't have another way to access the internet) to download the latest firmware for the router (go to http://www.cradlepoint.com/support/mbr95 and scroll over **firmware** at the bottom of the page). Then log in to the router administration pages and manually upload the firmware. Go to **System Settings → System Software** and click on "Manual Firmware Upload".

- If you are still unable to access the internet after following the above directions, contact CradlePoint Technical Support for further assistance.

3.3.2 You are Connected to the Router but Cannot Connect to the Internet

The status LEDs of your router will give you an indication whether or not a proper connection is being made. See the LED STATUS definitions below:

If the USB data modem LEDs are not illuminated, your modem is not connected and online. You may need to update firmware. Refer to the previous section, "~~Y~~our USB Modem Does Not Work With The Router."



If you are still not online after updating, call CradlePoint Technical Support for further assistance.

3.3.3 Your MBR95 router gets an IP conflict when you plug it into your Cable or DSL modem.

- If your Cable or DSL modem is not working with the router, check that there is not an IP conflict. Go to **Internet → Connection Manager** and find the Ethernet connection under WAN Interfaces. If it says —IP conflict" you will need to change the IP address of the MBR95 router from —192.168.0.1". A suggested IP address is —192.168.10.1".
- Change the IP address by going to **Network Settings→ WiFi / Local Network**. Find the IP address under —LAN Settings" and type the alternate IP address. Click **Apply** to save the settings.

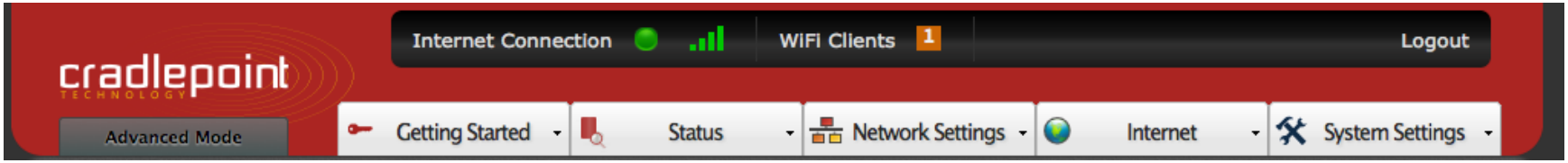
NOTE: To access the router administration pages after changing the IP address you will need to go to the new IP address in your internet browser instead of ~~http://~~192.168.0.1". You may continue to use ~~cp/~~" to access the router administration pages after this change.

If you are still unable to access the internet after following the above directions, contact CradlePoint Technical Support for further assistance.

4 WEB INTERFACE – ESSENTIALS

The MBR95 has a Web interface for configuration and administration of all features. The interface is organized with a button for toggling between **Basic Mode** and **Advanced Mode** and 5 tabs at the top of the screen:

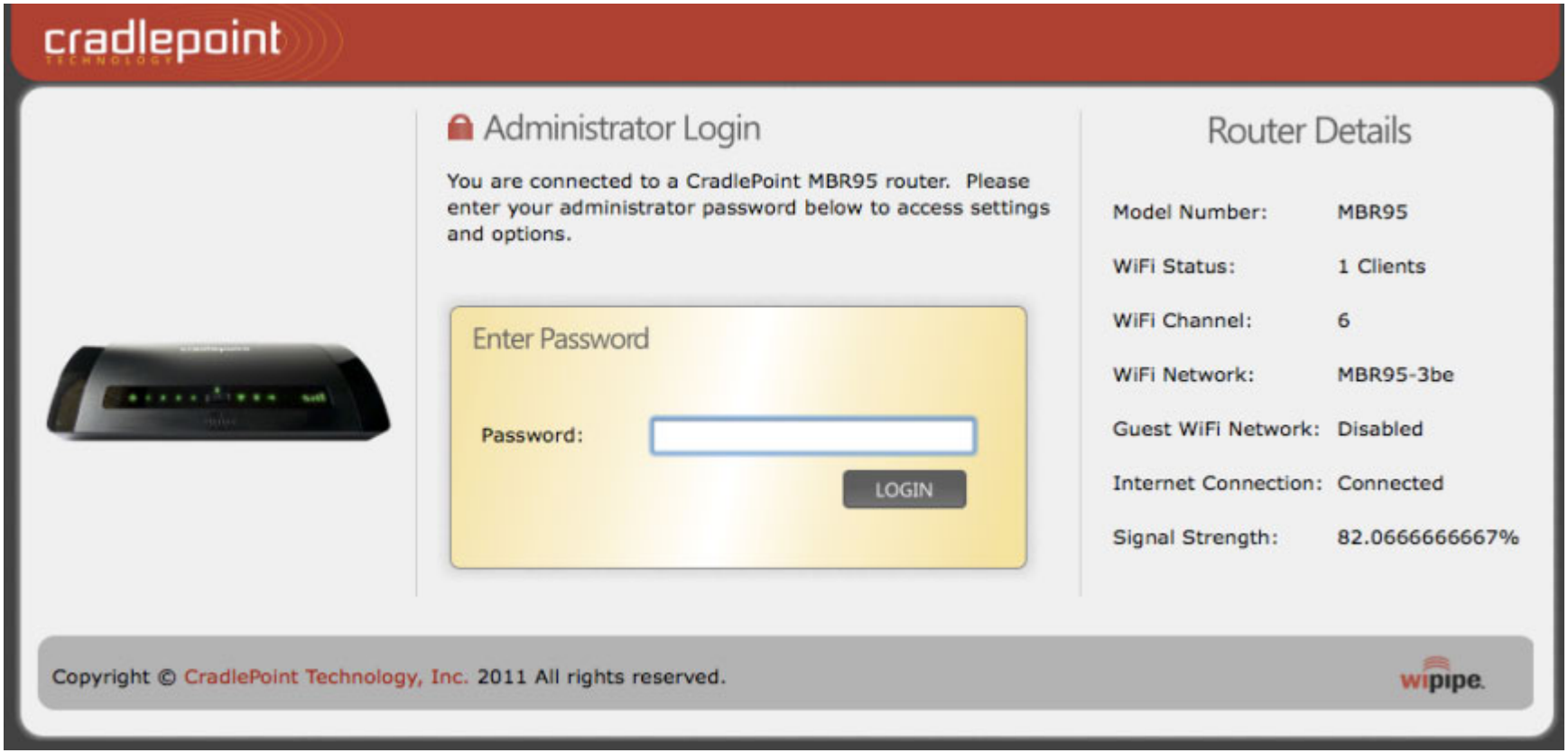
- Getting Started
- Status
- Network Settings
- Internet
- System Settings



Click on any of the 5 tabs to open a dropdown menu with further options for the administration of the MBR95.

4.1 *Administrator Login*

To access the administration pages, open a Web browser and type the hostname "~~cp/~~" or IP address "~~http://~~192.168.0.1" into the address bar. The Administrator Login page will appear.



Log in using your administrator password. Initially, this password can be found on the bottom of the MBR95 unit as the **Default Password**. This password is also the last eight digits of the unit's MAC address.

You may have changed the administrator password during initial setup using the First Time Setup Wizard. Log in using your personalized administrator password.

If you have forgotten your personalized password, you can reset the MBR95 to factory defaults. When you reset the router, the administrator password will revert back to the **Default Password**. Press and hold the **reset button** on the router unit until the lights flash (10 seconds). You can then log in using the **Default Password**.

4.1.1 Router Details

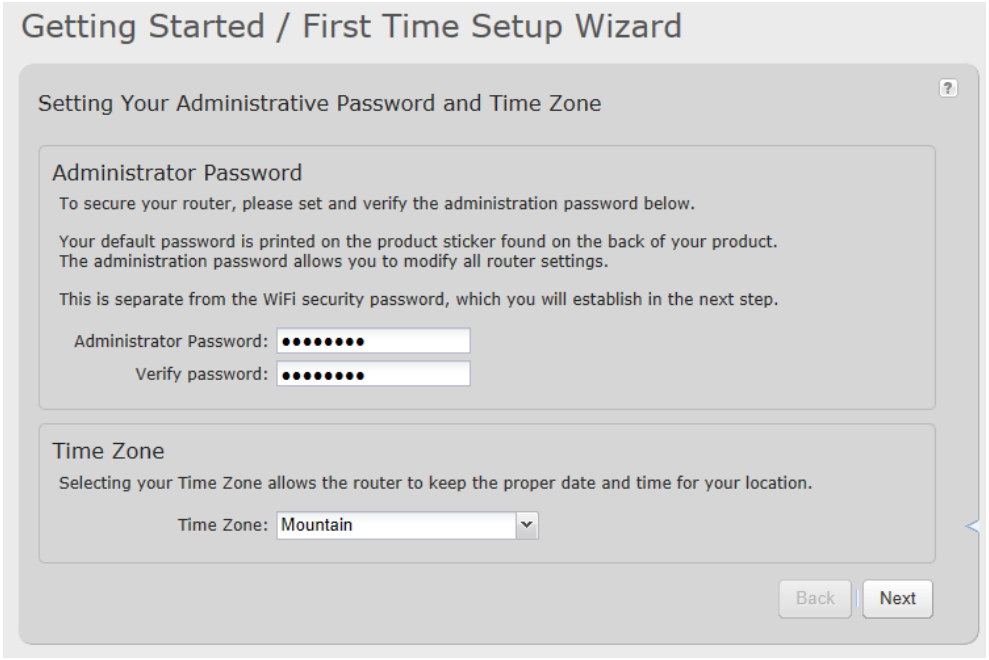
The Administrator Login page includes a section that shows the following **Router Details**:

- **Model Number:** MBR95
- **WiFi Status:** The number of clients.
- **WiFi Channel:** The channel number.
- **WiFi Network:** The name of the main network.
- **Guest WiFi Network:** ―Disabled" or, if enabled, the name of the guest network.
- **Internet Connection:** Connected/Disconnected
- **Signal Strength:** The strength of your internet connection, shown as a percentage.

4.2 *Getting Started – First Time Setup*

The **First Time Setup Wizard** will help you customize the name of your wireless network, change passwords to something you choose, and establish an optimal WiFi security mode. The MBR95 comes out of the box with a unique password at WPA1/WPA2 WiFi security level.

Note: Instructions for the **First Time Setup Wizard** are also located in the **Setup Guide** included with the MBR95.



1) Open a browser window and type "~~http://~~cp/" or "~~http://~~192.168.0.1" into the address bar. Press enter/return.

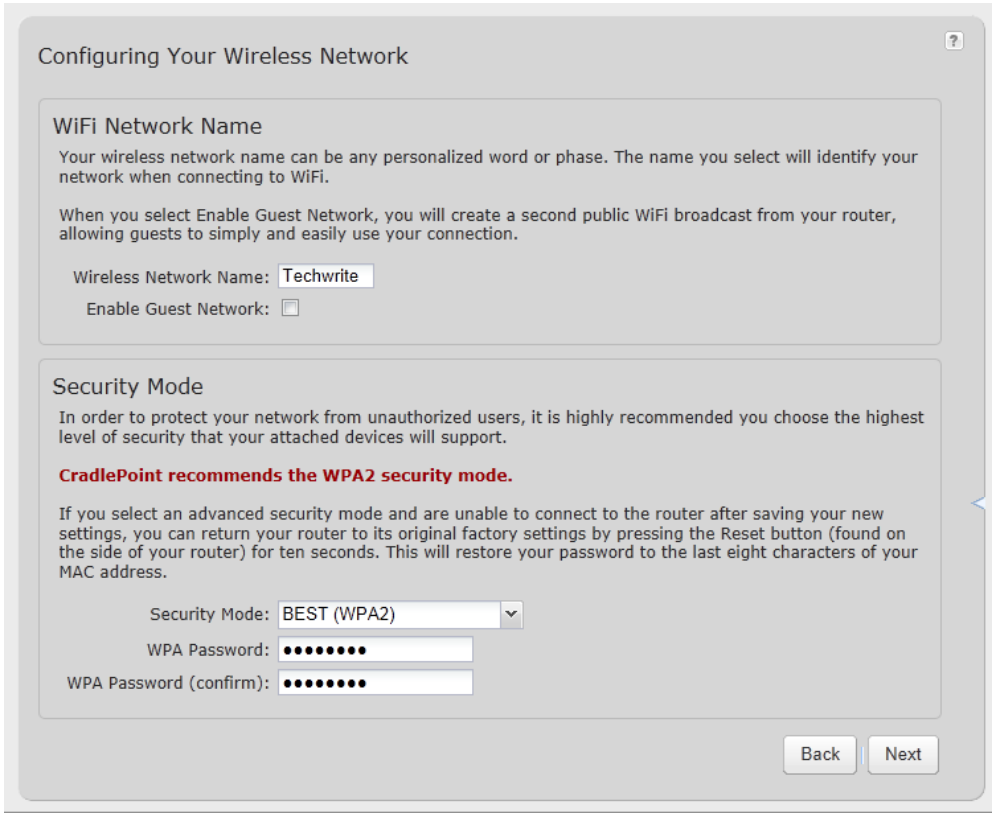
2) When prompted for your password, type the eight character **Default Password** found on the product label on the bottom of the MBR95 (this is also the last 8 digits of the router's MAC address).

3) When you log in for the first time, you will be automatically directed to the **FIRST TIME SETUP WIZARD**. (Otherwise, go to **Getting Started → First Time Setup**).

4) CradlePoint recommends that you change the router's **ADMINISTRATOR PASSWORD**, which is used to log in to the administration pages. The administrator password is separate from the WiFi security password, although initially the **Default Password** is used for both.

5) Select your **TIME ZONE** from the dropdown list. Click **NEXT**.

6) CradlePoint recommends that you customize your WiFi Network Name. Type in your personalized Network name here. You can also enable the Guest Network feature (for more configuration options, see **Network Settings → WiFi / Local Network** and the Wireless (WiFi) Network Settings section of this manual).



Choose the **WIFI SECURITY MODE** that best fits your needs:

- **BEST (WPA2):** Select this option if your wireless adapters support WPA2-only mode. This will connect to most new devices and is the most secure, but may not connect to older devices or some handheld devices such as a PSP.
- **GOOD (WPA1 & WPA2):** Select this option if your wireless adapters support WPA or WPA2. This is the most compatible with modern devices and PCs.
- **POOR (WEP):** Select this option if your wireless adapters only support WEP. This should only be used if a legacy device that only supports WEP will be connected to the router. WEP is insecure and obsolete and is only supported in the router for legacy reasons. The router cannot use 802.11n modes if WEP is enabled; WiFi performance and range will be limited.
- **NONE (OPEN):** Select this option if you do not want to activate any security features.

CradlePoint recommends BEST (WPA2) WiFi security. Try this option first and switch only if you have a device that is incompatible with WPA2.

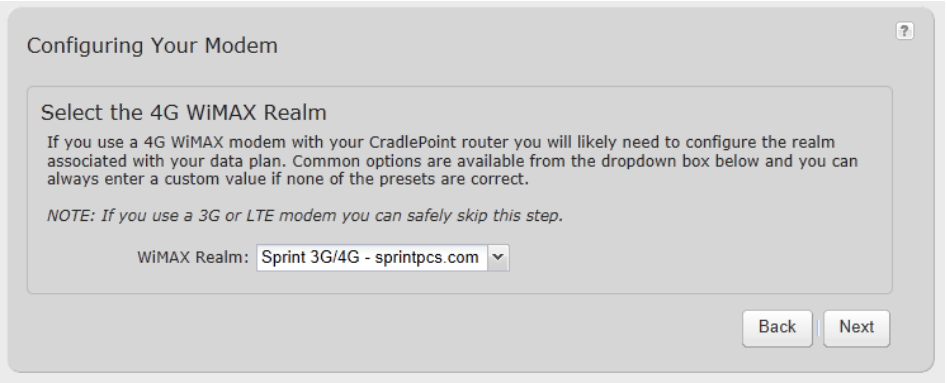
Choose a personalized **WPA PASSWORD** or **WEP KEY**. This password will be used to connect devices to the router's WiFi broadcast once the security settings have been saved.

WPA Password: The WPA Password must be between 8 and 64 characters long. A combination of upper and lower case letters along with numbers and special characters is recommended to prevent hackers from gaining access to your network.

WEP Key: A WEP Key must be either a hexadecimal value of 5 or 13 characters or a text value of 10 or 26 characters.

Click **NEXT**.

7) If you are using a 4G WiMAX modem, you will want to establish the Realm for your carrier. This setting ensures that the modem, when attached to the router, will properly connect to your carrier's wireless broadband service. The MBR95 will default to the Sprint Realm. Select your carrier from the dropdown menu (options shown below).



- Clear - clearwire-wmx.net
- Rover - rover-wmx.net
- Sprint 3G/4G - sprintpcs.com
- Xohm - xohm.com
- BridgeMAXX - bridgeMAXX.com
- Time Warner Cable - mobile.rr.com
- Comcast - mob.comcast.net

NOTE: If you use a 3G or LTE modem you can safely skip this step.

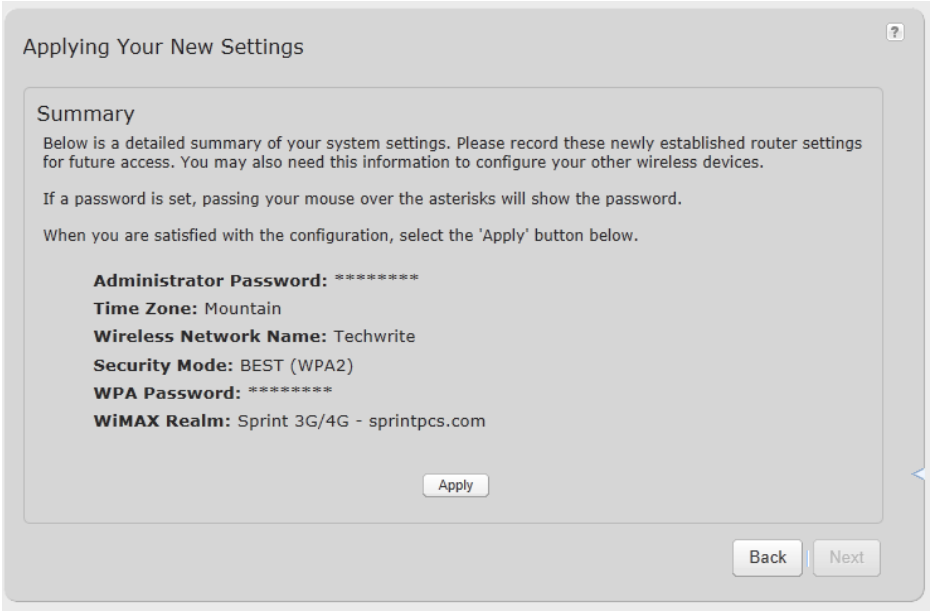
Click **NEXT**.

8) Review the details and record your wireless network name, administrative password, and WPA password (or WEP key). Move your mouse over the passwords to selectively reveal each password.

   Please record these settings for future access. You may need this information to configure other wireless devices.

   NOTE: If you are currently using the MBR95 WiFi network, reconnect your devices to the network using the new wireless network name and security password.

   Click **APPLY** to save the settings and update them to your router.



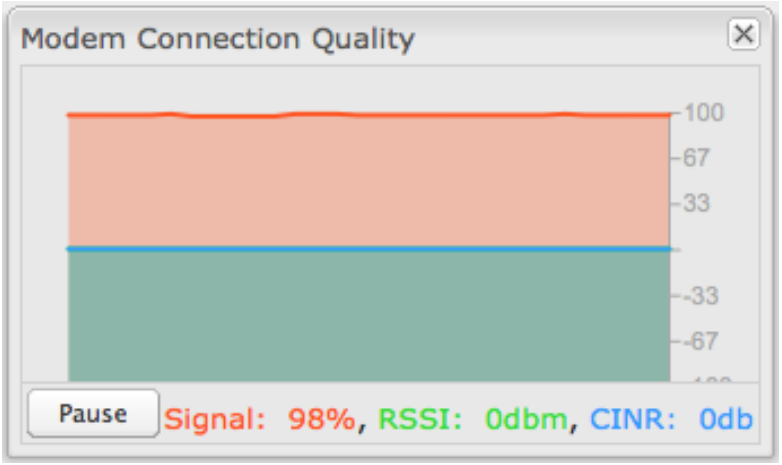
4.3 *Quick Links*

The CradlePoint logo in the upper left-hand corner of all the administration pages is a link to the Router Console (**Status → Router Console**), which displays fundamental information about the router.

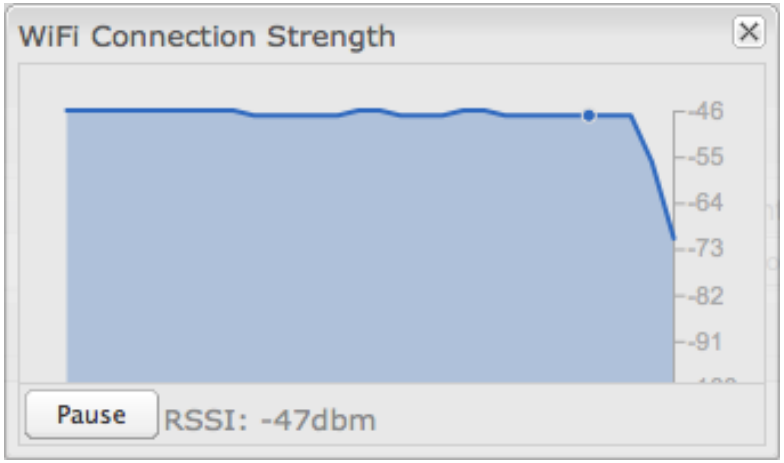
The black bar across the top provides quick access to important information and controls.

Internet Connection This links to the Connection Manager (**Internet → Connection Manager**) where you can manage your internet sources.

Click on the image of four signal bars to open a "Modem Connection Quality" popup window that shows the strength of your internet signal.



WiFi Clients Click to view a signal strength indicator for your network, "WiFi Connection Strength".



Logout Click to log out of the administration pages.

4.4 *Basic Mode vs. Advanced Mode*

For less complex uses, the MBR95 can be controlled within **Basic Mode**. Clicking on the **Basic Mode** button switches the complete Web interface to **Advanced Mode**. **Advanced Mode** provides several additional features.

The following chart shows the complete list of features found in **Basic Mode** and found exclusively in **Advanced Mode**:

	Getting Started	**Status**	**Network Settings**	**Internet**	**System Settings**
Basic Mode	First Time Setup WiFi Protected Setup	Client List GPS Router Console Internet Connections Statistics System Logs	Content Filtering MAC Filter WiFi / Local Network	Connection Manager Ethernet Settings Modem Settings	Administration System Control System Software
Advanced Mode (also includes all options in Basic Mode)			DHCP Server DNS Firewall Routing WiPipe QoS	WiFi as WAN Settings	Alerts Managed Services

Since **Advanced Mode** includes all features found in both modes, **ALL REMAINING INSTRUCTIONS IN THIS MANUAL WILL ASSUME YOU ARE IN ADVANCED MODE.**

If an expected feature is missing from the user interface, be sure to check that you are using **Advanced Mode**.

4.5 *Network Settings vs. Internet*

When using the Web interface, it will be important to pay attention to the difference between the **internet source** for your MBR95 and the **network** created by the MBR95. The **"Internet"** tab broadly refers to the router's source of internet, while the **"Network Settings"** tab broadly refers to the network created by the router.

The following chart highlights this difference:

Network Settings tab	**Internet** tab
Internet –output"	Internet –input"
Network created by MBR95	Source for MBR95
LAN (Local Area Network)	WAN (Wide Area Network)

Examples:

- If you want to change the content filtering settings for the network created by the MBR95, go to the **Network Settings** tab.
- If you have multiple internet sources (such as a USB modem and an Ethernet connection) for which you would like to set priority levels, go to the **Internet** tab.

5 STATUS

The Status tab *displays information*—no adjustments can be made from within this tab. It provides access to 7 submenu options:

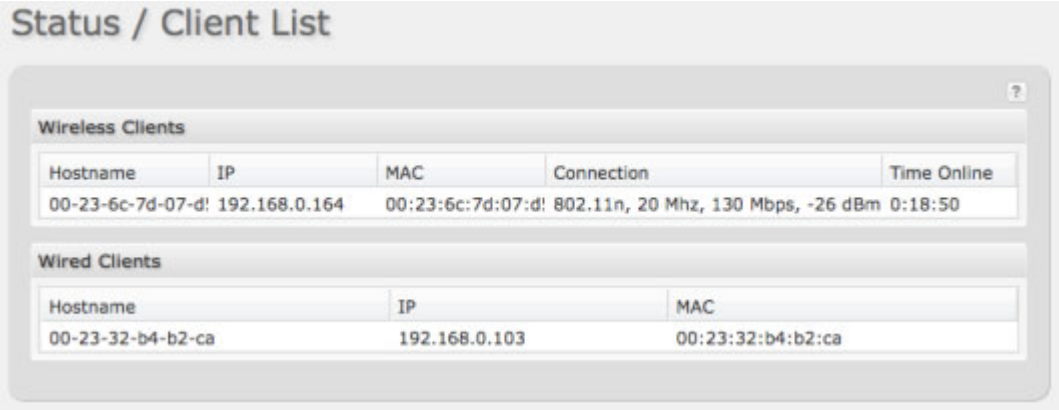
- Client List
- GPS
- Router Console
- Internet Connections
- Statistics
- System Logs

5.1 *Client List*

The Client List displays the specifications of each device connected to your router, including **Wireless** and **Wired** clients.

Wireless Clients. For each device using a wireless connection to your MBR95, the following information is displayed: **Hostname**, **IP**, **MAC**, **Connection**, and **Time Online**.

Wired Clients. For each device using a wired connection to your MBR95, the following information is displayed: **Hostname**, **IP**, and **MAC**.



Hostname: The name by which each computer or device in a network is known.

IP: The "IP address," or "Internet Protocol address," specifies a location for each device.

MAC: This is the "MAC address", a factory-assigned identifier used to identify a specific attached computer or device.

Connection: Summary of the wireless connection. For example: **802.11n, 20 MHz, 130 Mbps, -26 dBm**

- **802.11n:** The transmission standard being used by the client. Possible values include 802.11b, 802.11g, and 802.11n. 802.11n is the newest and best standard, but some older devices may not support it.
- **20 MHz:** This is the channel width that defines the theoretical data rate (in megahertz) that the attached computer or device can send to or receive from the router. The channel width is set in **Network Settings → WiFi / Local Network**. Typically this will be 20 MHz, but 40 MHz is possible if the router is set to use two adjacent 20 MHz channels. A wider channel can mean better performance, but not if there is too much interference.
- **130 Mbps:** The transmit rate (in megabits per second) currently used to transmit packets from the router to the client. This rate changes automatically to match environmental conditions. Distance from the router, interference, etc can impact this value. Higher values indicate better performance. Devices can still function in the network with as little as 1 Mbps.
- **-26 dBm:** A relative measure of wireless signal quality (decibels relative to one milliwatt). This expresses theoretical best quality. The value is given as a negative exponent: -20 is a very good value while -80 is relatively

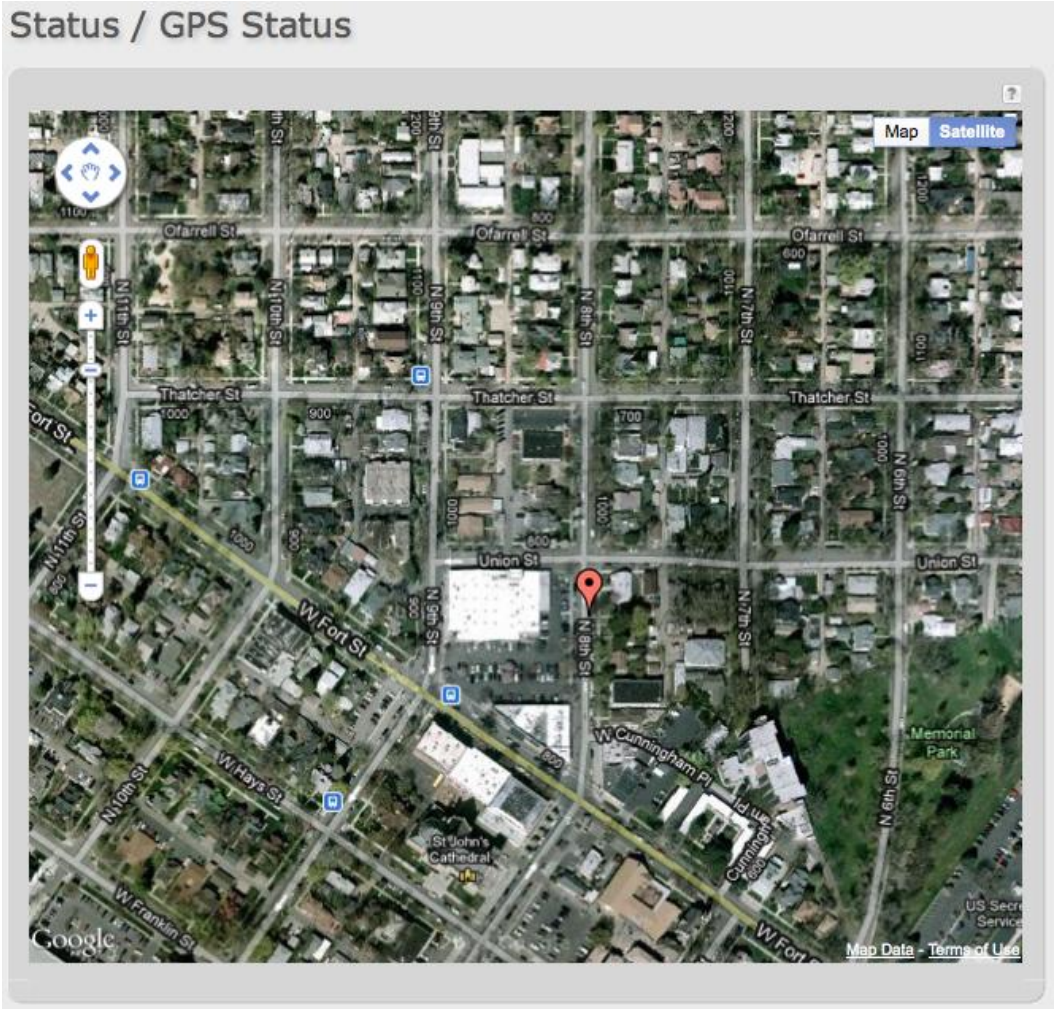
poor. Signal quality can be reduced by distance, by interference from other radio-frequency sources (such as cordless telephones or neighboring wireless networks), and by obstacles between the router and the wireless device.

Time Online: Simply the amount of time the device has been connected to the router.

5.2 *GPS*

If GPS support is enabled and a modem capable of providing GPS coordinates is connected, this page will show a graphical view of your router's location. See the GPS section in **System Settings → Administration** to enable GPS support.

GPS information is only displayed if 1) the modem supports GPS, 2) your carrier allows the GPS functionality, and 3) the modem has sufficient GPS signal strength. If no information is displayed, check that both the modem and your carrier support GPS.[1] If GPS is supported make sure the modem is in an area where it can receive a signal from the GPS satellites.



[1] By default, Sprint usually supports GPS on USB data modems and Verizon usually does not.

5.3 *Router Console*

The Router Console functions as a dashboard for the router, bringing various types of fundamental information together in one place. Once you have completed initial setup, every time you log in you will automatically be directed to this **Router Console** page. Also, clicking on the **CradlePoint** logo in the upper left-hand corner will redirect you to the Router Console page.

Included categories:

- **Router Information**
- **Internet**
- **Local Network**
- **WiFi Network**
- **System**.

More information can be found at the appropriate administration pages.

Router Information

- **Product:** MBR95
- **Date:** Year-month-day-hours-minutes-seconds for the most recent firmware upgrade.
- **Firmware**: Gives the number of the current firmware version.

To check for Firmware upgrades, see **System Settings → System Software**.

Internet

- **State:** Connected/Disconnected, active WAN type (Ethernet, Modem, etc.), signal strength.
- **IP Address**
- **Netmask**
- **Gateway**
- **DNS Servers**

To configure "State" see **Internet → Connection Manager**.
The IP address, netmask, and gateway describe your active WAN source.
To configure DNS servers see **Network Settings → DNS**.

Local Network

- **Hostname** (default: "ep")
- **IP Address**
- **Netmask**
- **DHCP Server:** Enabled/Disabled
- **WiPipe QoS:** Enabled/Disabled

To change hostname, IP address, or netmask see **Network Settings → WiFi / Local Network**.
For DHCP server options see **Network Settings → DHCP Server**.
To configure WiPipe QoS see **Network Settings → WiPipe QoS**.

WiFi Network

- **WiFi Radio:** Enabled/Disabled
- **Channel:** 1-11
- **Network Name**
- **Clients:** Number of clients.
- **Security:** WPA2/WPA1/WEP
- **Guest WiFi:** Disabled/Enabled. If Enabled, also shows:
  - **Guest Network Name**
  - **Guest Security**

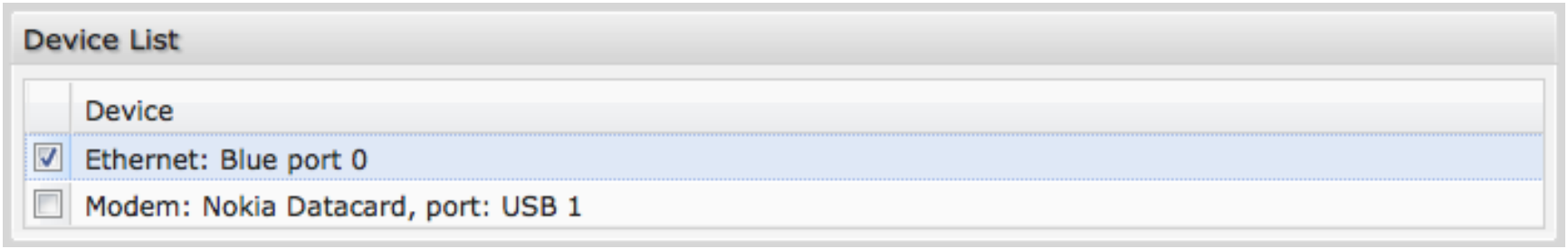
To configure WiFi network settings see **Network Settings → WiFi / Local Network**.

System

- **Up Time:** Total time for current session.
- **Load Average**
- **CPU Usage**
- **Time:** Current local time.

5.4 *Internet Connections*

The Internet Connections submenu option provides a list of attached WAN devices used as the internet source for the MBR95. Select one of these devices to see detailed information about that particular device.



For each type of device, different information will be included in the **Device Information** section. Possible devices include:

- Ethernet
- WiFi
- GSM Modem
- EVDO Modem
- WiMAX Modem
- LTE Modem

Depending on the device, possible information will be in the following sections: Diagnostics, General Information, IP Information, and Statistics. For modems, the Diagnostics section provides specific information about how the modem is communicating with its carrier.

5.4.1 Ethernet

Diagnostics

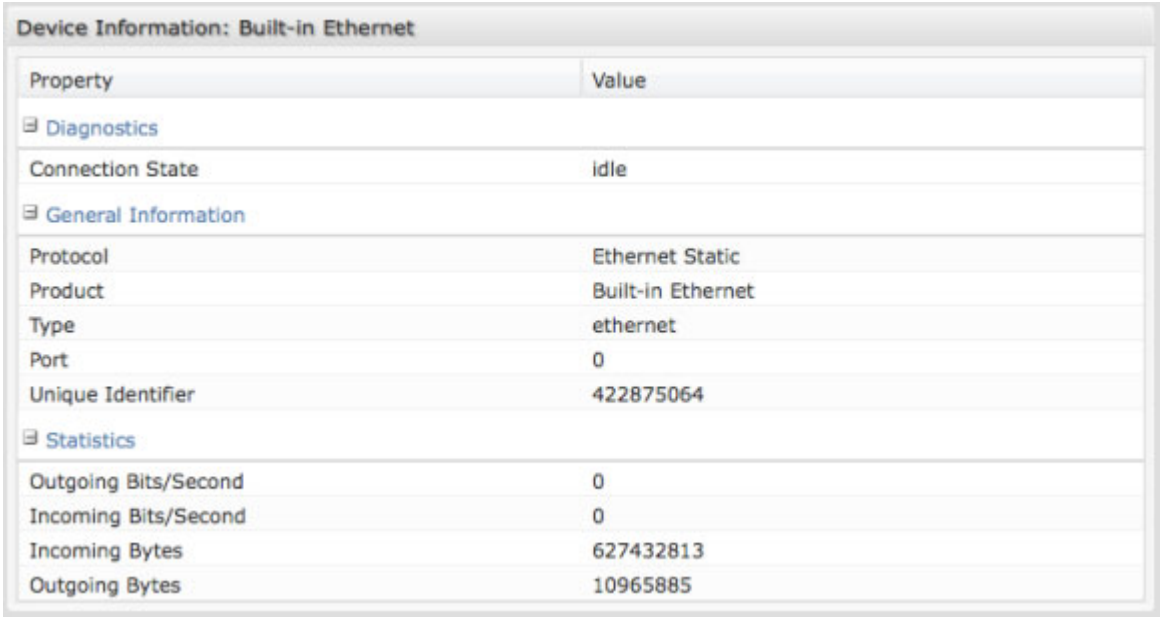
- **Connection State** (connected, idle, etc.)

General Information

- **Protocol** *Ethernet Static*
- **Product** *Built-in Ethernet*
- **Type** *Ethernet*
- **Port**
- **Unique Identifier**

Statistics

- **Outgoing Bits/Second**
- **Incoming Bits/Second**
- **Incoming Bytes**
- **Outgoing Bytes**



Device Information: Built-in Ethernet

Property	Value
Diagnostics	
Connection State	idle
General Information	
Protocol	Ethernet Static
Product	Built-in Ethernet
Type	ethernet
Port	0
Unique Identifier	422875064
Statistics	
Outgoing Bits/Second	0
Incoming Bits/Second	0
Incoming Bytes	627432813
Outgoing Bytes	10965885

5.4.2 WiFi as WAN

Diagnostics

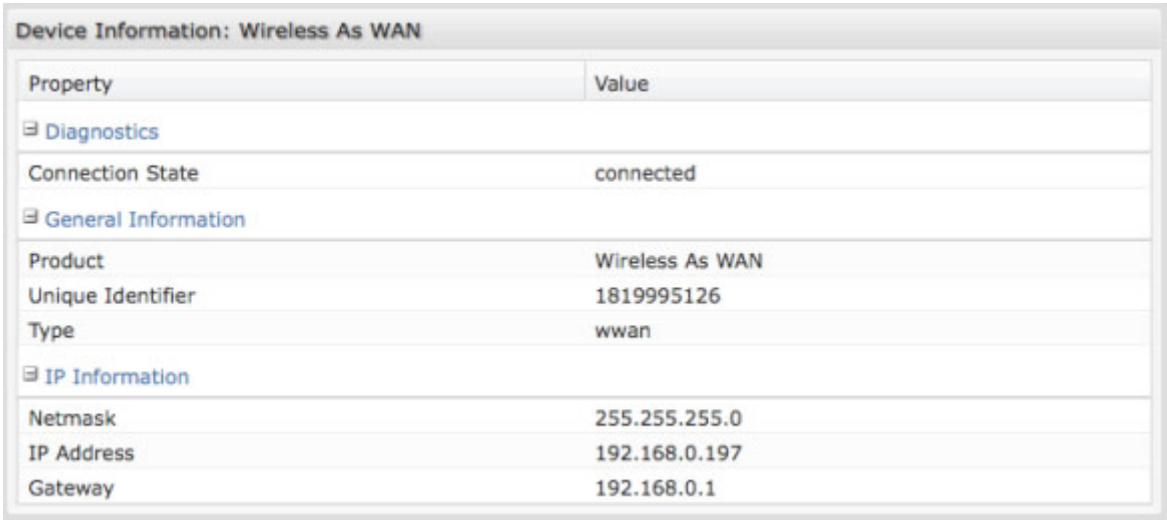
- **Connection State** (connected, idle, etc.)

General Information

- **Product** *Wireless As WAN*
- **Unique Identifier**
- **Type** *wwan*

IP Information

- **Netmask**
- **IP Address**
- **Gateway**



5.4.3 GSM Modem (Nokia Datacard)

Diagnostics

- **Signal Error Rate**
- **Modem Firmware Version**
- **Battery Status**
- **Battery Level**
- **Carrier Status**
- **Signal Strength(dBm)**
- **PIN Status**
- **Connection State** (connected, idle, etc.)

General Information

- **Product** *Nokia Datacard*
- **Protocol** *PPP*
- **Unique Identifier**
- **ESN/IMEI**
- **Model** *Nokia Internet Stick CS-18*
- **Type** *modem*
- **Port**
- **Manufacturer** *Nokia*

IP Information

- **Netmask**
- **IP Address**
- **Gateway**

Statistics

- **Outgoing Bits/Second**

Device Information: Nokia Datacard

Property	Value
Diagnostics	
Signal Error Rate	0
Modem Firmware Version	Modem mode
Battery Status	2
Battery Level	0
Carrier Status	UP
Signal Strength(dBm)	-65 dBm
PIN Status	READY
Connection State	connected
General Information	
Product	Nokia Datacard
Protocol	PPP
Unique Identifier	548307683
ESN/IMEI	[redacted]
Model	Nokia Internet Stick CS-18
Type	modem
Port	0
Manufacturer	Nokia
IP Information	
Netmask	255.255.255.0
IP Address	32.176.252.50
Gateway	10.0.0.1
Statistics	
Outgoing Bits/Second	0
Incoming Bits/Second	0
Incoming Bytes	36940
Outgoing Bytes	24704

- **Incoming Bits/Second**
- **Incoming Bytes**
- **Outgoing Bytes**

5.4.4 EVDO Modem: (MC760 Comcast)

Diagnostics

- **Modem Firmware Version**
- **PRL Version**
- **Service Display** *EVDO*
- **Carrier Status**
- **Signal Strength(dBm)**
- **Connection Type** *CDMA*
- **Connection State** (connected, idle, etc.)

General Information

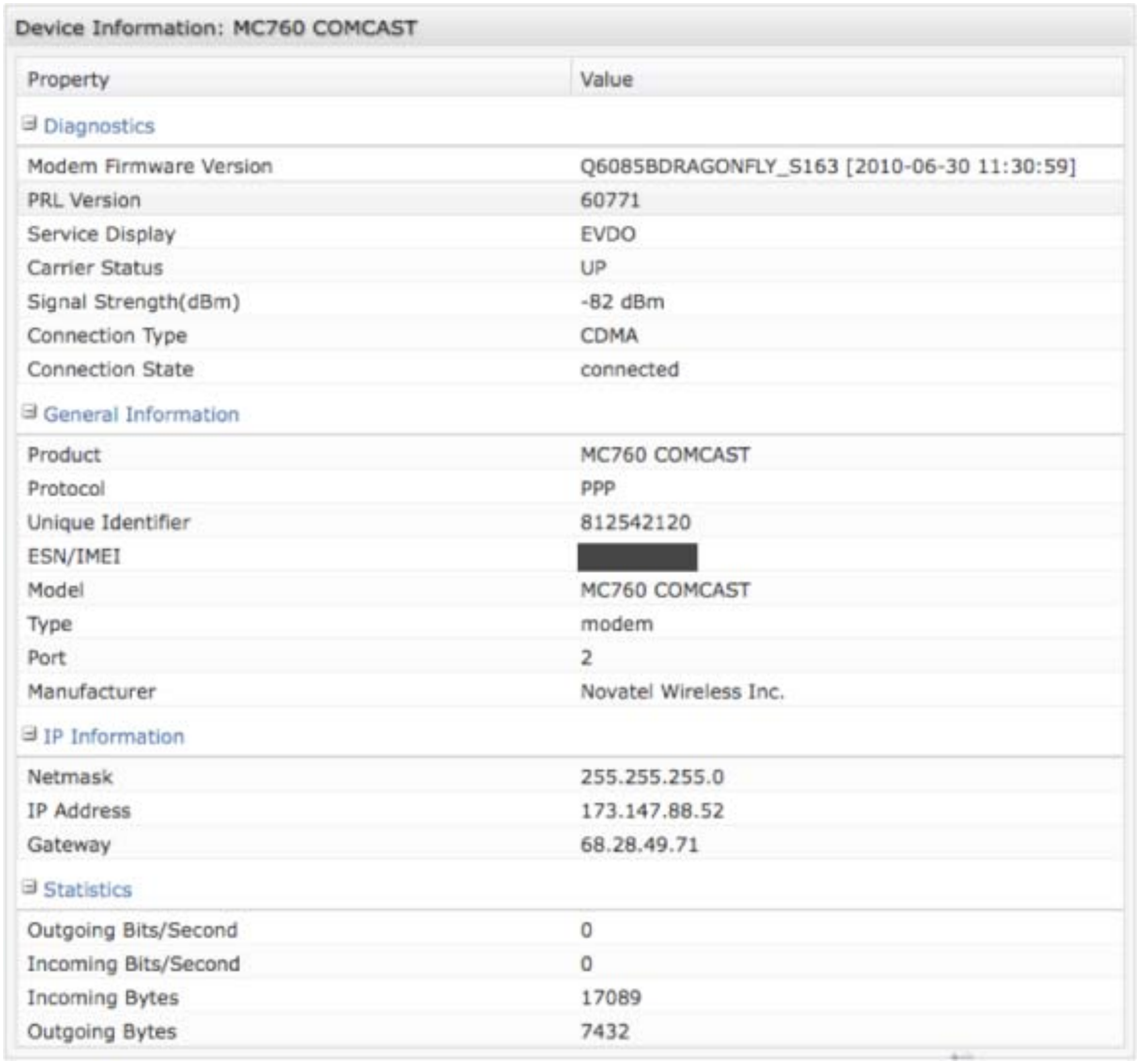
- **Product** *MC760 COMCAST*
- **Protocol** *PPP*
- **Unique Identifier**
- **ESN/IMEI**
- **Model** *MC760 COMCAST*
- **Type** *modem*
- **Port**
- **Manufacturer** *Novatel Wireless Inc.*

IP Information

- **Netmask**
- **IP Address**
- **Gateway**

Statistics

- **Outgoing Bits/Second**
- **Incoming Bits/Second**
- **Incoming Bytes**



Device Information: MC760 COMCAST

Property	Value
Diagnostics	
Modem Firmware Version	Q6085BDRAGONFLY_S163 [2010-06-30 11:30:59]
PRL Version	60771
Service Display	EVDO
Carrier Status	UP
Signal Strength(dBm)	-82 dBm
Connection Type	CDMA
Connection State	connected
General Information	
Product	MC760 COMCAST
Protocol	PPP
Unique Identifier	812542120
ESN/IMEI	[redacted]
Model	MC760 COMCAST
Type	modem
Port	2
Manufacturer	Novatel Wireless Inc.
IP Information	
Netmask	255.255.255.0
IP Address	173.147.88.52
Gateway	68.28.49.71
Statistics	
Outgoing Bits/Second	0
Incoming Bits/Second	0
Incoming Bytes	17089
Outgoing Bytes	7432

- **Outgoing Bytes**

5.4.5 WiMAX Modem (U300 – 4G)

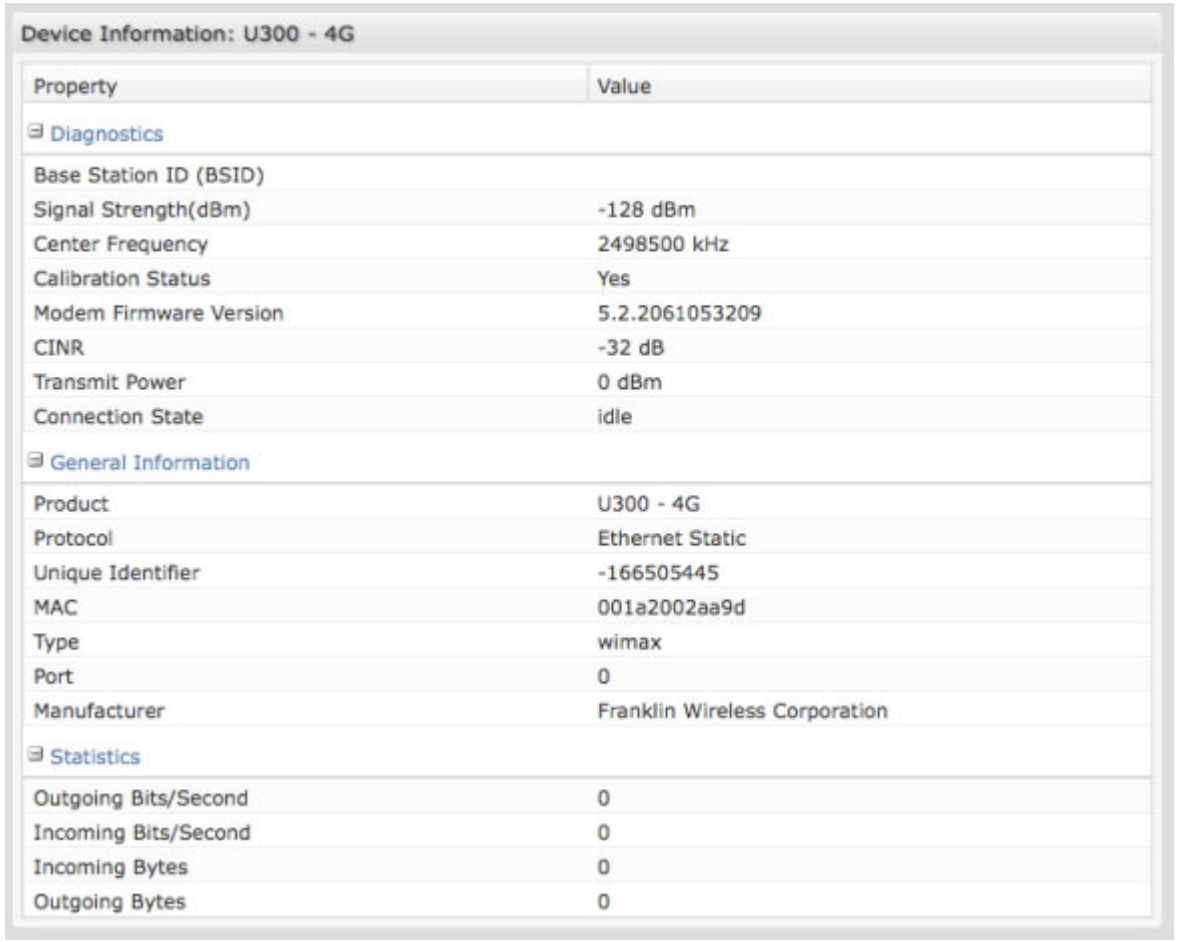
Diagnostics

For a WiMAX modem, the CINR and Signal Strength values are important as they show how strong the signal is and that has significant effects on how much data the router can download or send. You can place the router in different locations to see where you get better signal. You can also see a LED display of the current signal strength. Pressing the router's WPS button will toggle the LED display on and off.

- **Base Station ID (BSID)**
- **Signal Strength(dBm)**
- **Center Frequency**
- **Calibration Status**—Don't worry if this says the modem is not calibrated.
- **Modem Firmware Version**
- **CINR**
- **Connection State** (connected, idle, etc.)

General Information

- **Product** *U300 – 4G*
- **Protocol** *Ethernet Static*
- **Unique Identifier**
- **MAC**



Device Information: U300 - 4G

Property	Value
Diagnostics	
Base Station ID (BSID)	
Signal Strength(dBm)	-128 dBm
Center Frequency	2498500 kHz
Calibration Status	Yes
Modem Firmware Version	5.2.2061053209
CINR	-32 dB
Transmit Power	0 dBm
Connection State	idle
General Information	
Product	U300 - 4G
Protocol	Ethernet Static
Unique Identifier	-166505445
MAC	001a2002aa9d
Type	wimax
Port	0
Manufacturer	Franklin Wireless Corporation
Statistics	
Outgoing Bits/Second	0
Incoming Bits/Second	0
Incoming Bytes	0
Outgoing Bytes	0

- **Type** *WiMAX*
- **Port**
- **Manufacturer** *Franklin Wireless Corporation*

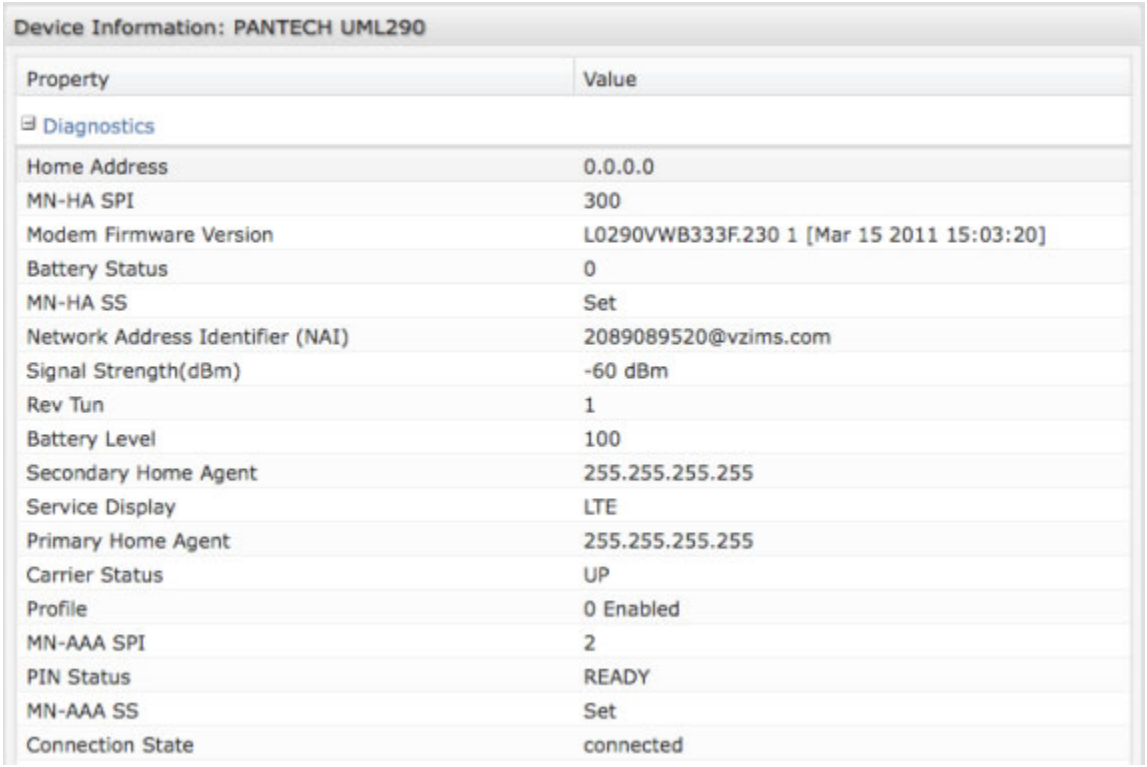
Statistics

- **Outgoing Bits/Second**
- **Incoming Bits/Second**
- **Incoming Bytes**
- **Outgoing Bytes**

5.4.6 LTE Modem (PANTECH UML290)

Diagnostics

- **Home Address**
- **MN-HA SPI**
- **Modem Firmware Version**
- **Battery Status**
- **MN-HA SS**
- **Network Address Identifier (NAI)**
- **Signal Strength(dBm)**
- **Rev Tun**
- **Battery Level**
- **Secondary Home Agent**
- **Service Display** *LTE*
- **Primary Home Agent**
- **Carrier Status**
- **Profile**
- **MN-AAA SPI**
- **PIN Status**
- **MN-AAA SS**
- **Connection State** (connected, idle, etc.)



Device Information: PANTECH UML290

Property	Value
Diagnostics	
Home Address	0.0.0.0
MN-HA SPI	300
Modem Firmware Version	L0290VWB333F.230 1 [Mar 15 2011 15:03:20]
Battery Status	0
MN-HA SS	Set
Network Address Identifier (NAI)	2089089520@vzims.com
Signal Strength(dBm)	-60 dBm
Rev Tun	1
Battery Level	100
Secondary Home Agent	255.255.255.255
Service Display	LTE
Primary Home Agent	255.255.255.255
Carrier Status	UP
Profile	0 Enabled
MN-AAA SPI	2
PIN Status	READY
MN-AAA SS	Set
Connection State	connected

General Information

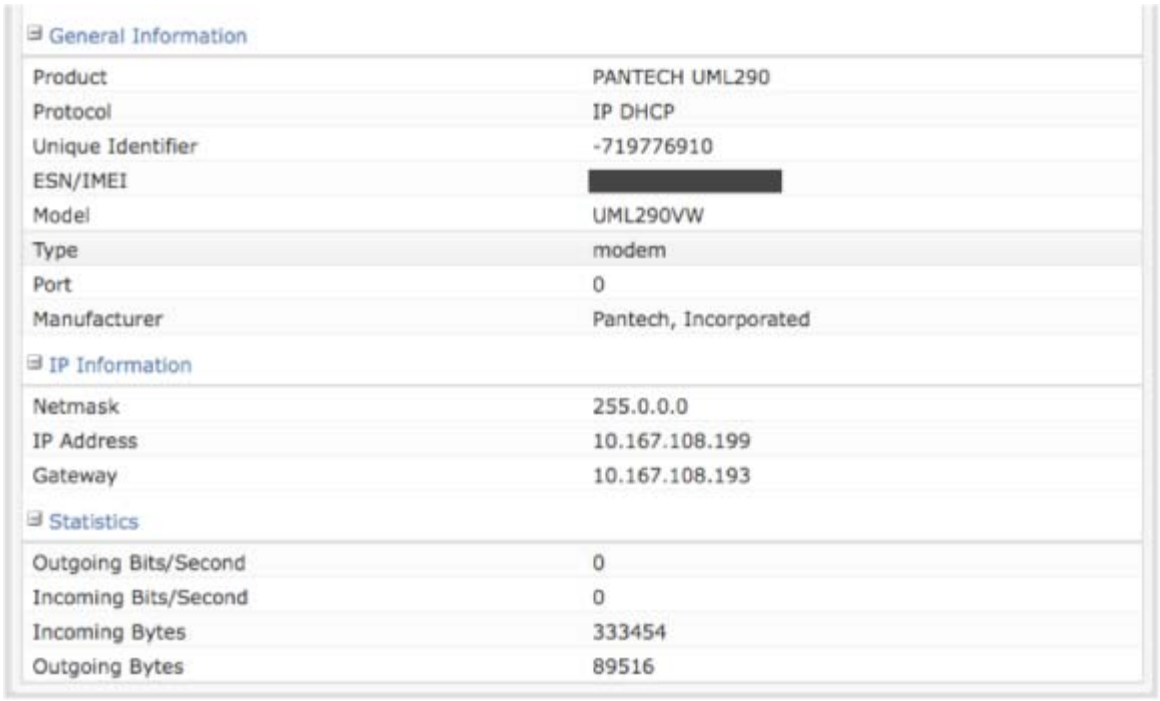
- **Product** *PANTECH UML290*
- **Protocol** *IP DHCP*
- **Unique Identifier**
- **ESN/IMEI**
- **Model** *UML290VW*
- **Type** *modem*
- **Port**
- **Manufacturer** *Pantech, Incorporated*

IP Information

- **Netmask**
- **IP Address**
- **Gateway**

Statistics

- **Outgoing Bits/Second**
- **Incoming Bits/Second**
- **Incoming Bytes**
- **Outgoing Bytes**



General Information	
Product	PANTECH UML290
Protocol	IP DHCP
Unique Identifier	-719776910
ESN/IMEI	[redacted]
Model	UML290VW
Type	modem
Port	0
Manufacturer	Pantech, Incorporated
IP Information	
Netmask	255.0.0.0
IP Address	10.167.108.199
Gateway	10.167.108.193
Statistics	
Outgoing Bits/Second	0
Incoming Bits/Second	0
Incoming Bytes	333454
Outgoing Bytes	89516

5.5 *Statistics*

The Statistics submenu option displays basic traffic statistics for both LAN and WAN connections, separating Outgoing Traffic and Incoming Traffic.

Data Rate: A measure of the amount of information that is currently being sent or received through the network.

Data: A measure of the total amount of information that has been sent or received.

Packets: The number of network packets that have been sent or received.

Errors: The number of network packets that failed to be sent or received.

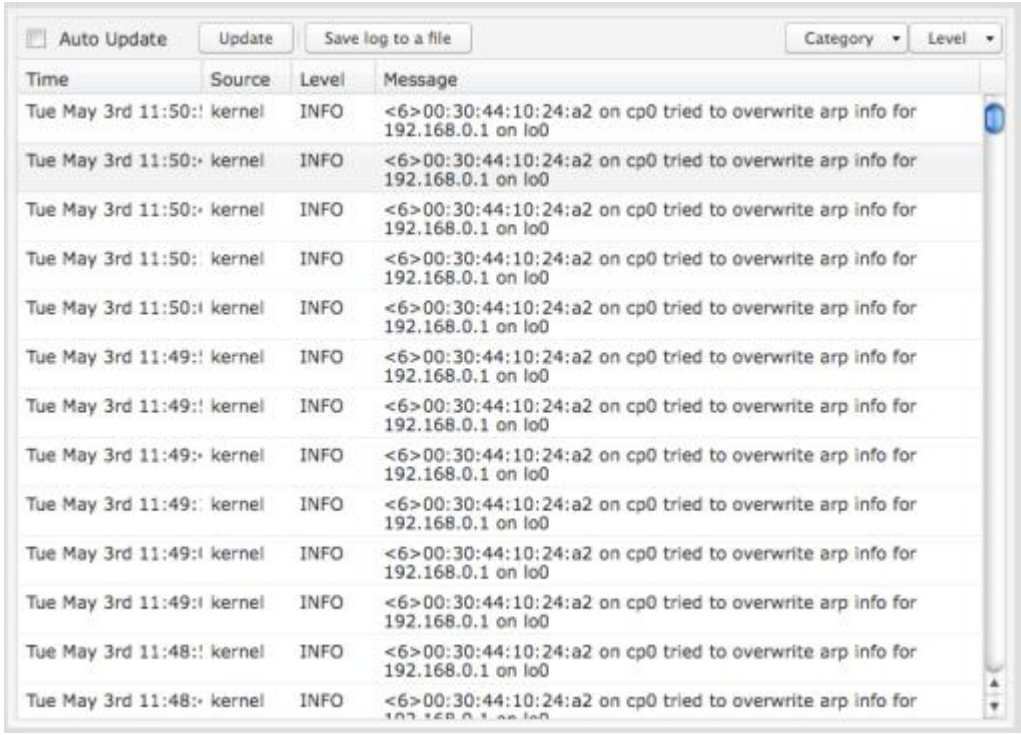
NOTE: Data, Packets, and Errors statistics include only the numbers since the router was most recently turned on or reset, not lifetime for the router.

Reset All: Press this button to zero all statistics. Counting restarts immediately.

Reminder: LAN vs. WAN

- **LAN**, or **Local Area Network**, is the network you have created through the MBR95.
- **WAN**, or **Wide Area Network**, is the internet source the MBR95 is using to create a new LAN. Possible WAN sources include: Ethernet, WiFi, USB modems, and ExpressCard modems.

5.6 *System Logs*



The router automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained. The log options allow you to filter the router logs you want to view. You can define what types of events you want to view and the level of events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

Auto Update: The logs automatically refresh whenever the router creates a new message.

Update: Click to check for new router messages.

Save log to a file: This will open a dialog in your browser that will allow you to save the router's log to your computer.

Category: Select to filter messages by category.

- Security & Authorization
- Router Status
- System Events

Level: Select to filter messages by priority.

- Critical
- Warning
- Info

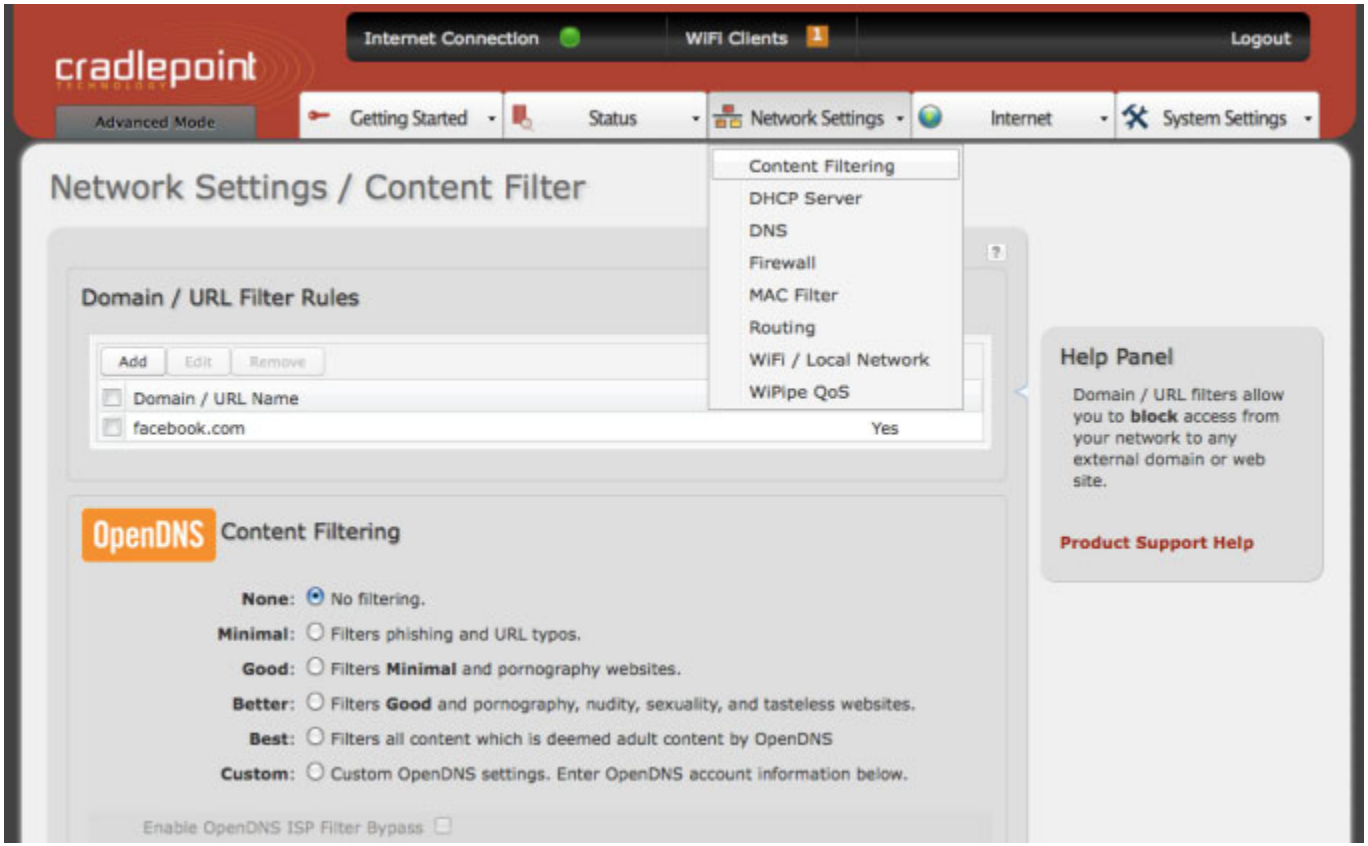
NOTE: The logs are erased whenever the router is rebooted or loses power.

6 NETWORK SETTINGS

The Network Settings tab provides access to 8 submenu options for administering the following functions/tasks. These functions are all related to controlling the LAN (Local Area Network), the network you set up with the MBR95.

- Content Filtering
- **DHCP Server**
- **DNS**
- **Firewall**
- MAC Filter
- **Routing**
- WiFi / Local Network
- **WiPipe QoS**

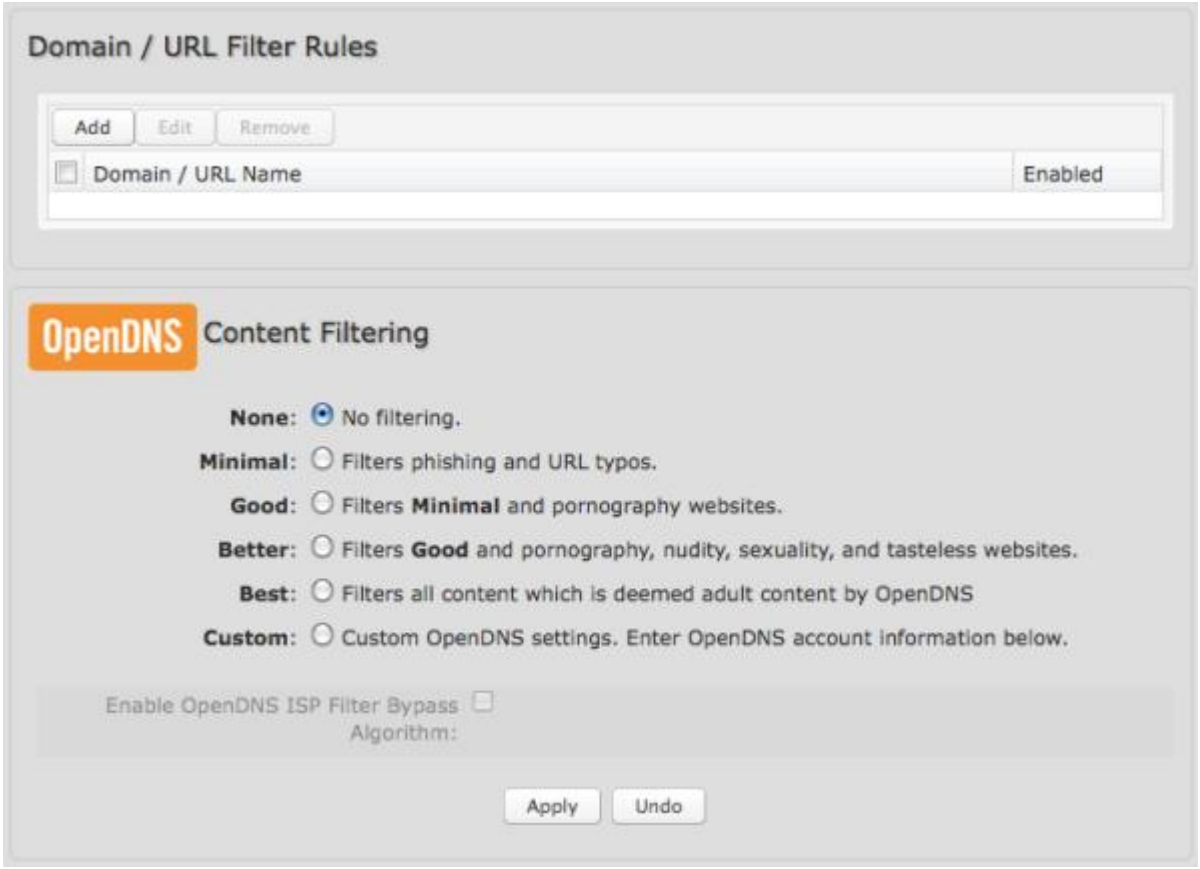
(**DHCP Server, DNS, Firewall, Routing,** and **WiPipe QoS**: Advanced Mode only)



6.1 *Content Filtering*

You have two main options for filtering content in the network created through your MBR95.

1) **Domain / URL Filter Rules:** Create a list of disallowed websites (facebook.com, for example).
2) **OpenDNS Content Filtering:** Allows several options for filtering rules.



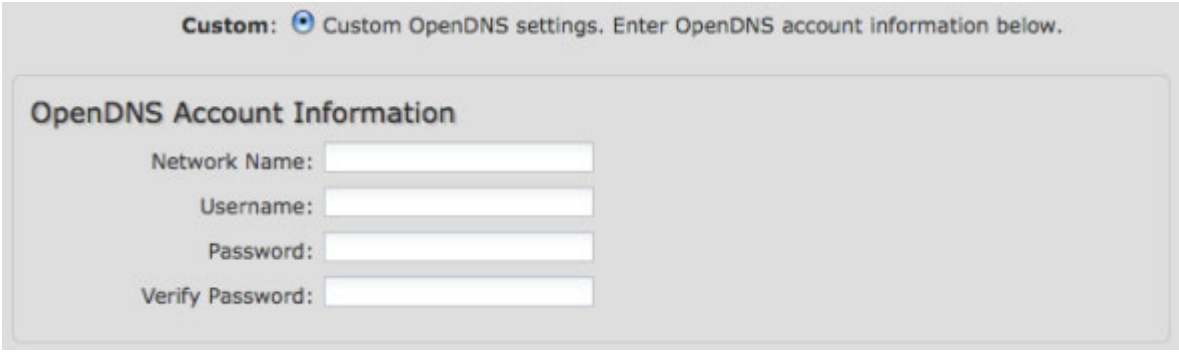
6.1.1 OpenDNS

OpenDNS is a service that protects you online by filtering websites. OpenDNS protects you from phishing websites and URL typos once you select a filtering level.

- **None:** Disables Web filtering that uses OpenDNS,
- **Minimal:** Filters phishing and URL typos.
- **Good:** Filters any Web site containing pornography and enables typo and phishing redirection.
- **Better:** Filters more nudity, sexuality, and tasteless content.
- **Best:** Filters more nudity, sexuality, and tasteless content. Selecting —Best" will filter all content which is deemed adult content by OpenDNS
- **Custom:** Custom OpenDNS settings. See below for more information.

In addition to the standard filtering levels, you have the following options for filter control:

Custom OpenDNS: To use the Custom OpenDNS setting you need to first create an OpenDNS account. You can create an account at OpenDNS and click on the ―Create Account" link. Follow the onscreen instructions to create an account.



Once you have an OpenDNS account, enter your account information in order to use your Custom OpenDNS settings. Custom OpenDNS settings use the DNS-O-MATIC (an OpenDNS Service) API to update the IP address of your OpenDNS network. In order for Custom settings to work you need to login to DNS-O-MATIC using your OpenDNS credentials and "Add A Service" for the network specified above.

Enable OpenDNS ISP Filter Bypass Algorithm: It is possible that your Internet Service Provider (ISP) uses the port that OpenDNS is configured to access, port 53, which will prevent OpenDNS filtering. If OpenDNS does not appear to be working correctly, enabling this will attempt to bypass those ports when using an OpenDNS content filtering level.

6.2 *DHCP Server (Advanced Mode only)*

DHCP stands for Dynamic Host Configuration Protocol. The built-in DHCP Server automatically assigns IP addresses to the computers and other devices on your local area network (LAN) and Wireless local area network (WLAN). In this section, you have options for configuring the DHCP Server and controlling some of its features.

Enable DHCP Service: (Default: Enabled) When the DHCP Server is enabled, users of your network will be able to automatically connect to the internet without any special configuration. **It is recommended that you leave this enabled.** Disabling the DHCP Server is only recommended if you have another DHCP Server on your network and it is configured properly.

Starting and ending IP addresses: These designate the range of values in the reserved pool of IP addresses for the DHCP Server. Values within this range will be given to any DHCP enabled computers on your network. The default values are almost always sufficient (default: 192.168.0.72 to 192.168.0.200).

Example: The MBR95 uses an IP address of 192.168.0.1. A computer designated as a Web server has a static IP address of 192.168.0.3. Another computer is designated as an FTP server with a static IP address of 192.168.0.4. The starting IP address for the DHCP server needs to be 192.168.0.5 or higher.

Lease Time: [Default: 720 minutes (12 hours)] The lease time specifies how long DHCP enabled computers will wait before requesting a new DHCP lease. Smaller values are better suited to busy environments.

Active Leases: A list of devices that have been provided DHCP leases. The DHCP Server automatically assigns these leases. This list will not include any devices that have static IP addresses on the network.

Reservations: This option lets you reserve IP addresses and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the router. The router will provide the device the same IP address every time. DHCP Reservations are helpful for server computers on the local network that are hosting applications such as Web and FTP. Servers on your network should either use a static IP address or use a reservation.

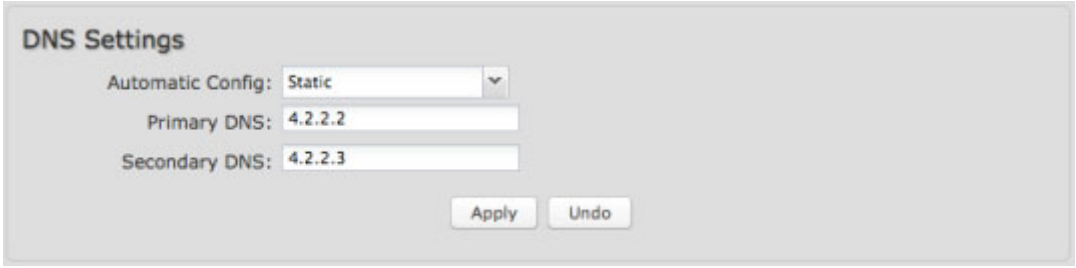
While you have the option to manually input the information to reserve an IP address (Hostname, Hardware Addr, IP Addr), it is much simpler to select a device under the **Active Leases** section and click "**Reserve**." The selected device's information will automatically be added under **Reservations**.

6.3 *DNS (Advanced Mode only)*

DNS, or Domain Name System, is a naming system that translates between domain names (www.cradlepoint.com, for example) and internet IP addresses (206.207.82.197). A DNS server acts as an internet phone book, translating between names that make sense to people and the more complex numerical identifiers. The DNS page for the MBR95 has these distinct functions:

- **DNS Settings:** By default your router is set to automatically acquire DNS servers through your internet provider (Automatic). **DNS Settings** allows you to specify DNS servers of your choosing instead (Static).
- **Dynamic DNS (DynDNS) Configuration:** Allows you to host a server (Web, FTP, Game Server, etc.) using a domain name that you have purchased (www.yourname.com) with your dynamically assigned IP address.
- **Known Hosts Configuration:** Allows you to map a name (xbox, nas, toaster, etc.) to an IP address of a device on the network.

6.3.1 DNS Settings



You have the option to choose specific DNS servers for your network instead of using the DNS servers assigned by your internet provider. The default DNS servers are usually adequate. You may want to assign DNS servers if the default DNS servers are performing poorly, if you want WiFi clients to access DNS servers that you use for customized addressing, or if you have a local DNS server on your network.

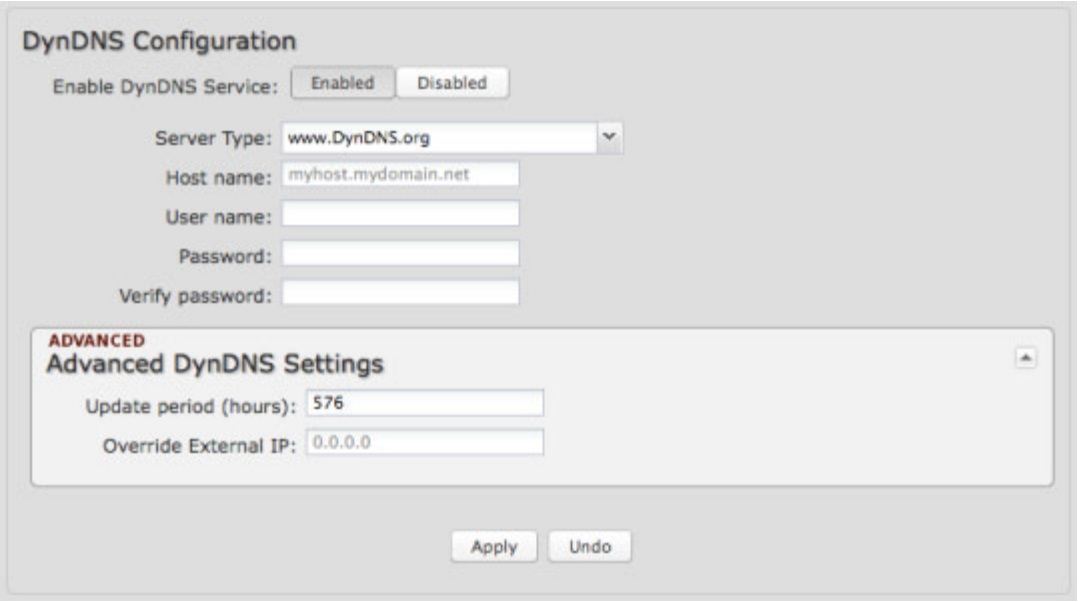
Automatic Config: Automatic or Static (default: Automatic). Switching to —Static” enables you to set specific DNS servers in the **Primary DNS** and **Secondary DNS** fields.

Primary DNS and **Secondary DNS:** If you choose to specify your DNS servers, then enter the IP addresses of the servers you want as your primary and secondary DNS servers in these fields.

For example, Google Public DNS servers have the IP addresses 8.8.8.8 and 8.8.4.4 while 4.2.2.2 and 4.2.2.3 are servers from Level 3 Communications.

6.3.2 DynDNS Configuration

The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc.) using a domain name that you have purchased (www.yourname.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. When you use a Dynamic DNS service provider, you can enter your host name to connect to your server, no matter what your IP address is.



Enable DynDNS Service: Enable this option only if you have purchased your own domain name and registered with a Dynamic DNS service provider.

Server Type. Select a Dynamic DNS service provider from the pull-down list:

- www.DynDNS.org
- www.DNSomatic.com
- www.ChangeIP.com
- www.NO-IP.com
- Custom Server (DynDNS clone)

Custom Server Address. Only available if you select Custom Server from the Server Address dropdown list. Enter your custom dynamic DNS server address here. The server must support the DynDNS protocol. See www.dyndns.org for details. Example: **myserver.mydomain.net**.

Host name: Enter your host name, fully qualified. For example: **myhost.mydomain.net**.

User name: Enter the user name or key provided by the Dynamic DNS service provider. If the Dynamic DNS provider supplies only a key, enter that key for both the **User name** and **Password** fields.

Password: Enter the password or key provided by the Dynamic DNS service provider.

6.3.3 Advanced DynDNS Settings

Update period (hours). (Default: 576) The time between periodic updates to the Dynamic DNS, if your dynamic IP address has not changed. The timeout period is entered in hours so valid values are from 1 to 8760.

Override External IP. The external IP is usually configured automatically during connection. However, in situations where the unit is within a private network behind a firewall or router, the network's external IP address will have to be manually configured in this field.

You may find out what your external IP address is by going to http://myip.dnsomatic.com/ in a web browser.

6.3.4 Known Hosts Configuration

The Known Hosts Configuration feature allows you to map a name (xbox, nas, toaster, etc.) to an IP address of a device on the network. This assigns a new hostname that can be used to conveniently identify a device within the network, such as an office printer.

Click **Add** to name a device in your network.

Fill in the following fields:

- **Hostname:** Choose a name that is meaningful to you. No spaces are allowed in this field.
- **IP address:** The address of the device within your network.

For example, a personal laptop with IP address 192.168.0.164 could be assigned the name —MyLaptop".

Since the assigned name is mapped to an IP address, the device's IP address should not change. To ensure that the device keeps the same IP address, go to the

—Reservations" section under **Network Settings → DHCP Server** and reserve the IP address for the device.

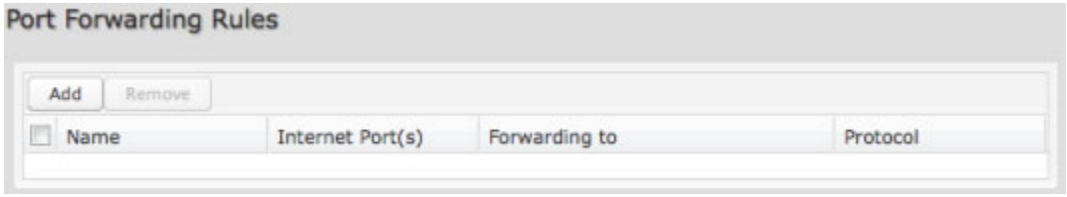
6.4 *Firewall (Advanced Mode only)*

The router automatically provides a firewall. Unless you configure the router to the contrary, the router does not respond to unsolicited incoming requests on any port, thereby making your LAN invisible to cyber attackers.

However, some network applications, such as some internet gaming systems, cannot run with a tight firewall. Those applications need to selectively open ports in the firewall to function correctly. The options on this page control ways of opening the firewall to address the needs of specific types of applications.

6.4.1 Port Forwarding Rules

A port forwarding rule allows traffic from the internet to reach a computer on the inside of your network. For example, a port forwarding rule might be used to run a Web server.



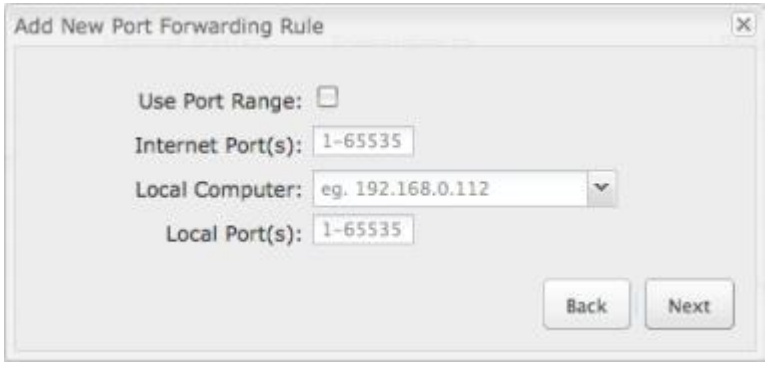
Exercise caution when adding new rules as they impact the security of your network.

Click **Add** to create a new port forwarding rule.

Add New Port Forwarding Rule: page 1

- **Name:** Name your rule.
- **Description:** Enter a short description of this rule for future reference.
- Click "**Next**" to continue.

Add New Port Forwarding Rule: page 2



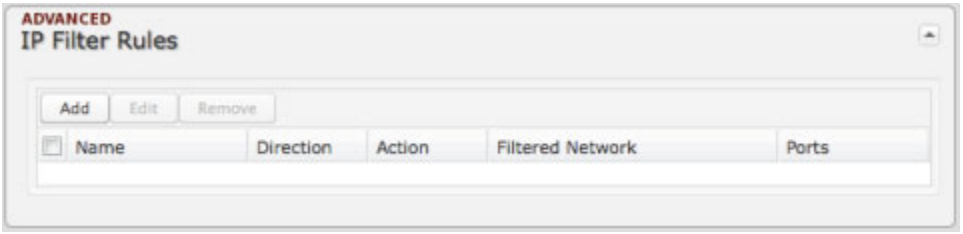
- **Use Port Range:** Changes the selection options to allow you to input a range of ports (if desired).
- **Internet Port(s):** The port number(s) as you want it defined on the internet. Typically these will be the same as the local port numbers, but they do not have to be. These numbers will be mapped to the local port numbers.
- **Local Computer:** Select the IP address of an attached device from the dropdown menu, or manually input the IP address of a device.
- **Local Port(s):** The port number(s) that corresponds to the service (Web server, FTP, etc) on a local computer or device.

  For example, you might input —80" in the **Local Port(s)** field to open a port for a Web server on a computer within your network. The **Internet Port(s)** field could then also be 80, or you could choose another port number that will be used across the internet to access your Web server. If you choose a number other than 80 for the internet Port, connections to that number will be mapped to 80—and therefore the Web server—within your network.

Add New Port Forwarding Rule: page 3

- **Protocol:** Select from the following options in the dropdown menu:
  - TCP
  - UDP
  - TCP & UDP
- Click **Add Rule** to save your completed port forwarding rule.

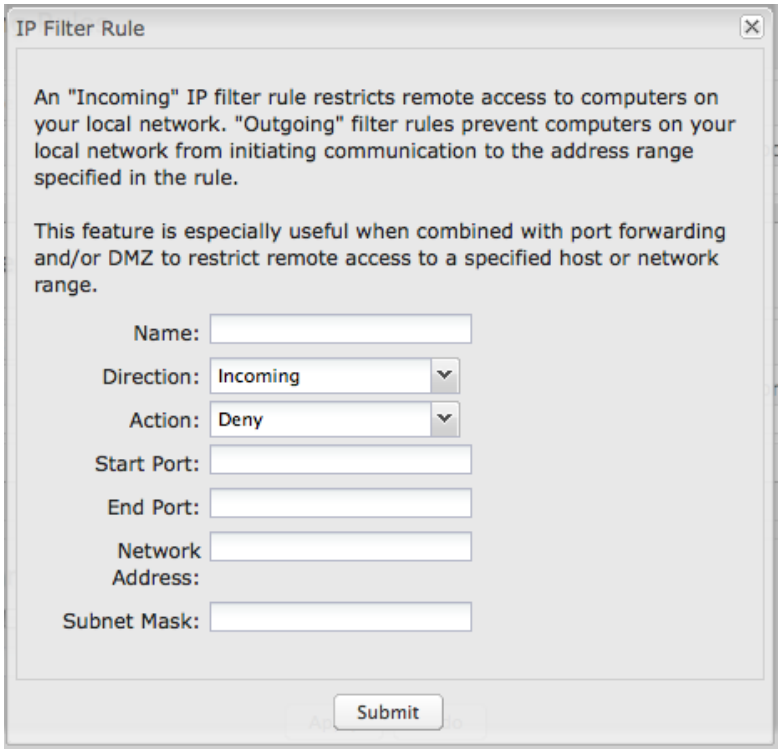
6.4.2 IP Filter Rules



An "Incoming" IP filter rule restricts remote access to computers on your local network. "Outgoing" filter rules prevent computers on your local network from initiating communication to the address range specified in the rule.

This feature is especially useful when combined with port forwarding and/or DMZ to restrict remote access to a specified host or network range. For example, you might have opened ports in order to host a gaming server with a port forwarding rule that could expose your LAN to cyber attacks. With an incoming IP filter rule, you can restrict the access to your LAN to only the computers of friends who have been invited to join your game.

- **Name:** Name your rule.
- **Direction:** —Incoming" or "Outgoing"
- **Action:** —Allow" or —Deny"
- **Start Port:** Use for a single port or a range of ports.
- **End Port:** Use for a single port or a range of ports.
- **Network Address**
- **Subnet Mask**



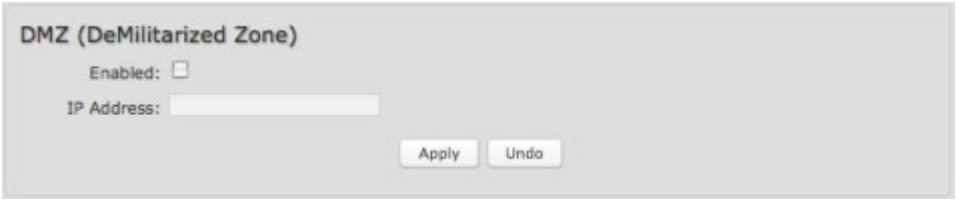
Use **Start Port**, **End Port**, **Network Address**, and **Subnet Mask** to specify the ports and addresses for which the rule applies. You can specify a range of ports or a single port (by inputting the same value in both port fields). Similarly, the subnet mask can be used to define either a range of addresses (i.e. 255.255.255.0) or a single address (255.255.255.255).

Example of an IP Filter Rule: Suppose you have opened a port in your firewall in order to run a server. Someone, Johnny, is abusing that opening, so you would like to restrict his access. Create a rule that will deny Johnny's IP address.

- **Name:** No more Johnny
- **Direction:** Incoming
- **Action:** Deny

- **Start Port:** 80
- **End Port:** 80
- **Network Address:** 172.22.24.160 (Johnny's IP address)
- **Subnet Mask:** 255.255.255.255 (This subnet mask restricts the rule to one single address).

6.4.3 DMZ (DeMilitarized Zone)



A DMZ host is effectively not firewalled in the sense that any computer on the internet may attempt to remotely access network services at the DMZ IP address. Typical uses involve running a public Web server, supporting older games, or sharing files.

Input the **IP Address** of a single device in your network to create a DeMilitarized Zone for that device. To ensure that the IP address of the selected device remains consistent, go to the —Reservations" section under **Network Settings → DHCP Server** and reserve the IP address for the device.

As with port forwarding caution should be used when enabling the DMZ feature as it can threaten the security of your network. DMZ should only be used as a last resort.

6.4.4 Firewall Options

Anti-Spoof: Anti-Spoof checks help protect against malicious users faking the source address in packets they transmit in order to either hide themselves or to impersonate someone else. Once the user has spoofed their address they can launch a network attack without revealing the true source of the attack or attempt to gain access to network services that are restricted to certain addresses.

Packet Normalization: Normalizing packets helps secure the router in untrusted environments. It does so by "scrubbing" packets that are ambiguous or might represent a break-in attempt. Packet Normalization also helps insure reliable connectivity for some WAN devices such as WiMAX modems. Only disable this option if you are sure you do not need it.

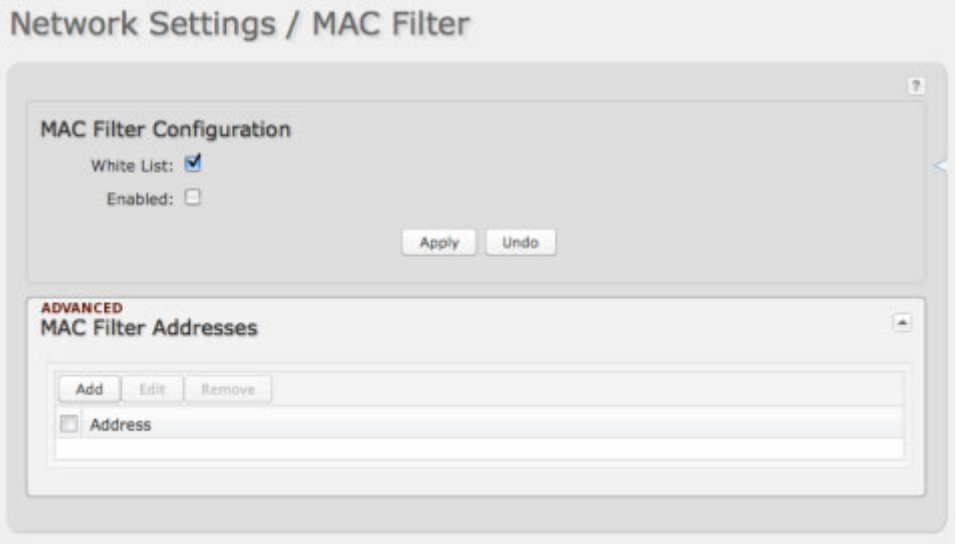
Static NAT Ports: If enabled the source port does not translate in TCP and UDP packets during NAT. Some NAT traversal protocols such as STUN(T) require that the source port stay the same when traversing the firewall.

6.5 *MAC Filter*

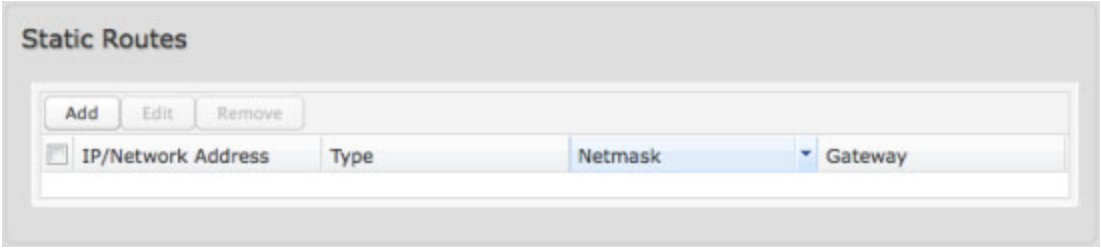
The MAC Filter allows you to create a list of devices that have either exclusive access (white list) or no access (black list) to your wireless LAN.

By default, the list of addresses is designated a —white list.” Deselecting White List turns the list of addresses into a disallowed black list.

Advanced: Add devices to either your white list or black list simply by inputting each device‘s MAC address.



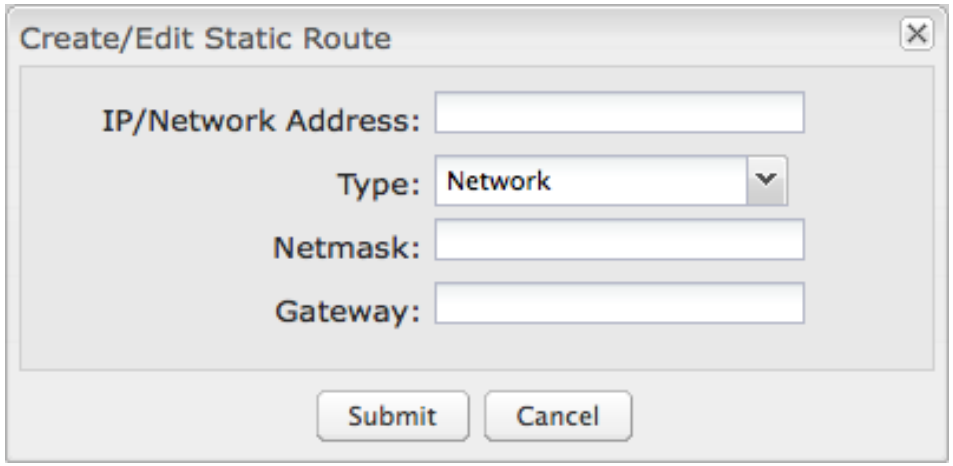
6.6 *Routing (Advanced Mode only)*



Add a new static route to the IP routing table or edit/remove an existing route.

Static routes are unnecessary for most users. They are typically only used in networks with more than one layer, such as when there is a network within a network so that packet destinations are hidden behind an additional router. Adding a static route is a way of telling the router about an additional step that packets will need to take to reach their destination.

Click **Add** to create a new static route.



IP/Network Address: The IP address of the target network or host.

Type: Select from a dropdown list to specify the type of the target:

- Network
- Host

Netmask: Used to specify which portion of the IP/Network Address signifies the network trying to be accessed and which part signifies the host that the packets will be routed to.

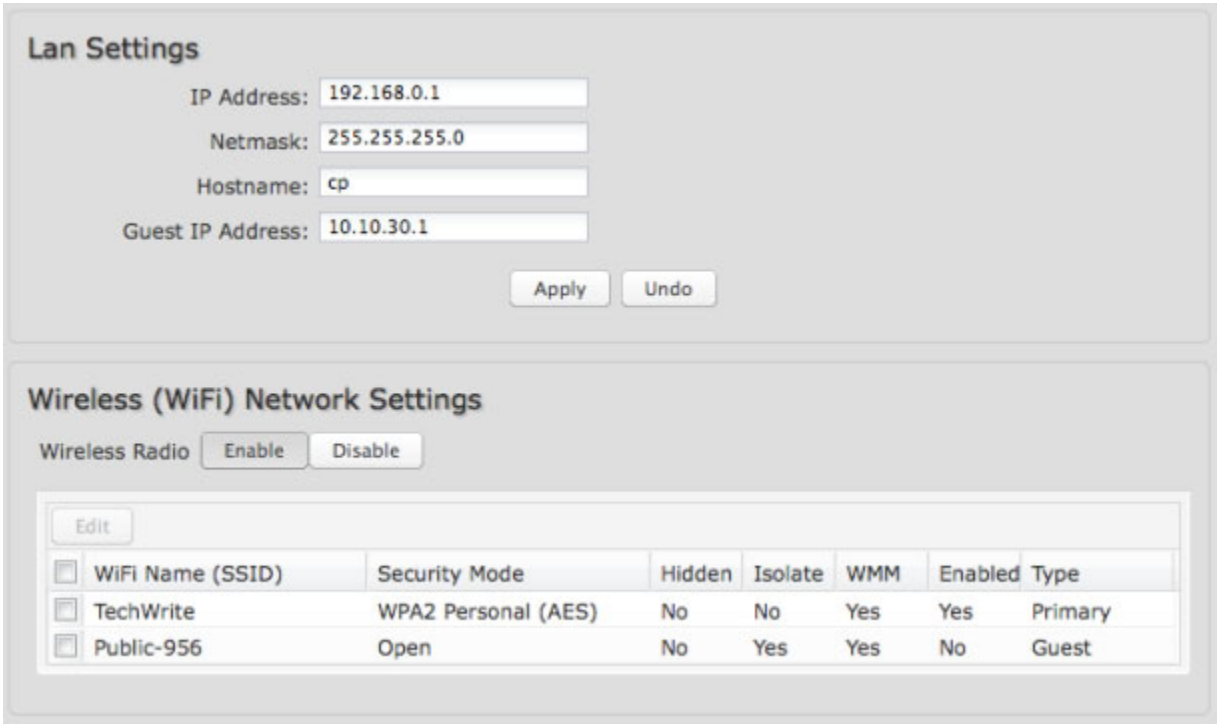
NOTE: 255.255.255.255 is used to signify only the host that was entered in the IP/Network Address field.

Gateway: Specifies the next hop to be taken if this route is used. A gateway of 0.0.0.0 implies there is no next hop, and the IP address matched is directly connected to the router on the interface specified: **LAN** or **WAN**.

6.7 *WiFi / Local Network*

This section is used to configure the settings for wireless networks created by your router. Note that changes made in this section may also need to be duplicated on wireless devices that you want to connect to your wireless network.

For example, if you change the LAN IP address, devices within your network will lose connection to the LAN. They will have to reconnect to your network.



6.7.1 LAN Settings

IP Address: This is the address used by the router for local area network communication. Changes to this parameter may require a restart to computers on this network.

Netmask: (Default: 255.255.255.0) The netmask controls how many IP addresses can be used in this network. The default value allows for 254 IP addresses, which is enough in most cases.

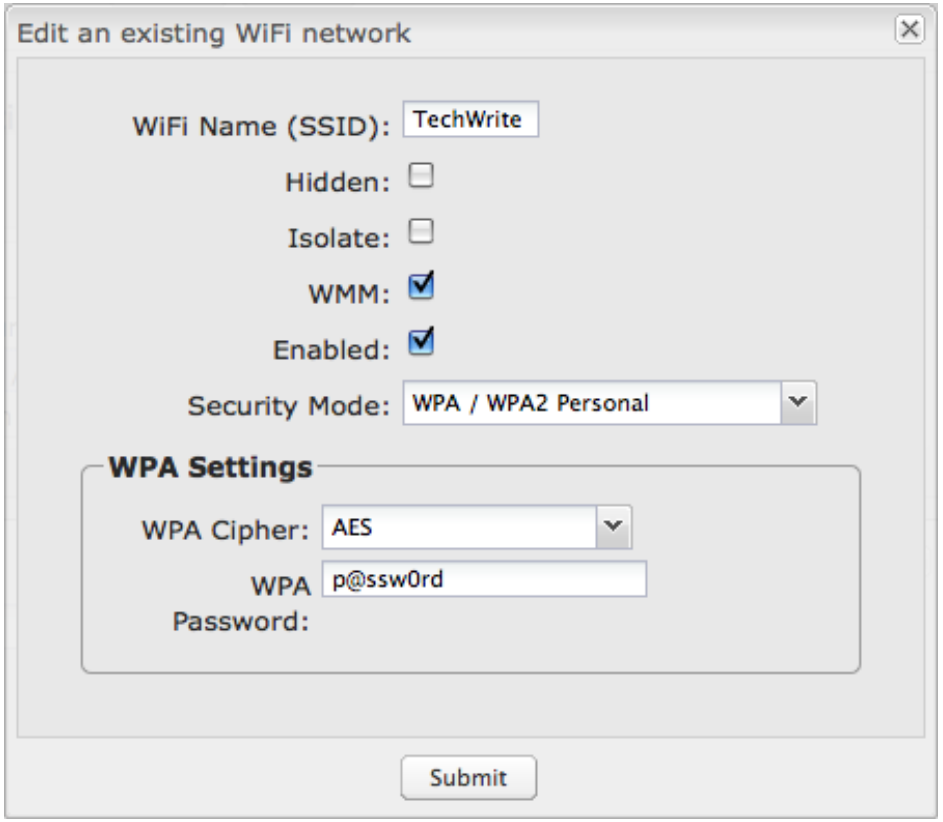
Hostname: [Default: cp (for CradlePoint)] The hostname is the DNS name associated with the router's local area network IP address. You can access the router‘s administration pages by inputting the hostname into your browser, so if you change “cp” to another hostname, you can access the administration pages through the new hostname.

Guest IP Address: This is the address used by the router for the guest network communication. The guest network DHCP range is automatically selected based off this address. The guest network cannot overlap with the main network.

6.7.2 Wireless (WiFi) Network Settings

By default, the MBR95 has two wireless networks set up: Primary and Guest. "Primary" is the main network for this router. "Guest" is an additional network that you may enable (this is disabled by default) to allow other people to briefly use your internet connection without knowing your Primary security password. It may have different security modes than your Primary network. Users on the Guest network can see other Guest connections and the internet, but cannot see devices on your Primary network.

Select either your Primary or Guest network. Click **Edit** to view the options to configure that network.



WiFi Name (SSID): When you are browsing for available wireless networks, this is the name that will be broadcast from this router for the selected network. This name is referred to as the SSID (service set identifier). For security purposes, it is highly recommended that you change this from the pre-configured name.

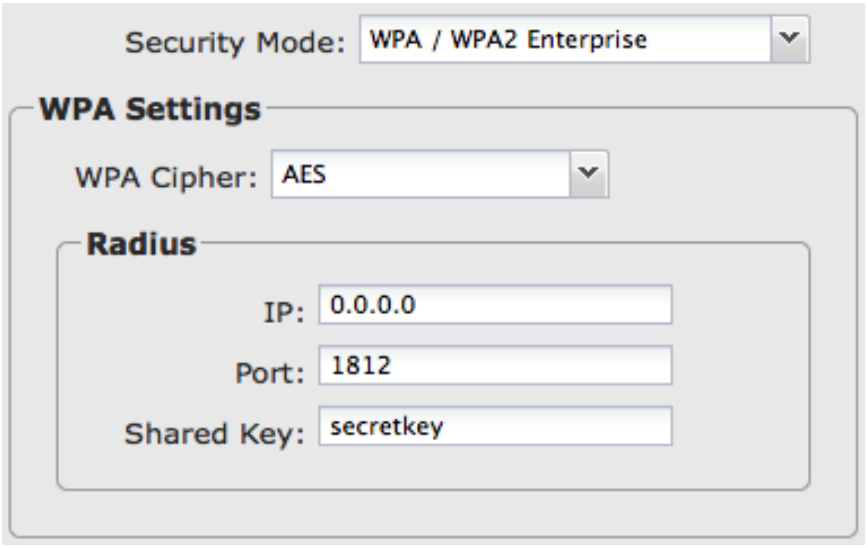
Hidden: This shows whether the router broadcasts its SSID. It is somewhat harder for hackers to find and attack a router that is not broadcasting its SSID, which adds to the wireless security.

Isolate: Select this to isolate all wireless clients so they cannot directly communicate with each other on the wireless network.

WMM: WiFi Multimedia. This is a basic traffic shaping, or QoS (quality of service), system for the network. WMM works behind the scenes to set priorities for different types of traffic on your network. For example, video streams are given higher priority than print jobs, since video streams need consistent throughput.

Enabled: If the network is available.

Security Mode: You have several options for selecting a security mode. The mode you choose depends on the security features your wireless adapters support. If you select one of the security modes and are unable to connect to the router afterwards, you can use the reset buttons to reset the router to its factory default state and try a different security mode instead.



- WPA2 Personal
- WPA / WPA2 Personal
- WPA Personal
- WPA2 Enterprise
- WPA / WPA2 Enterprise
- WPA Enterprise
- WEP Auto
- Open

Depending on which Security Mode you select, there are different setup options.

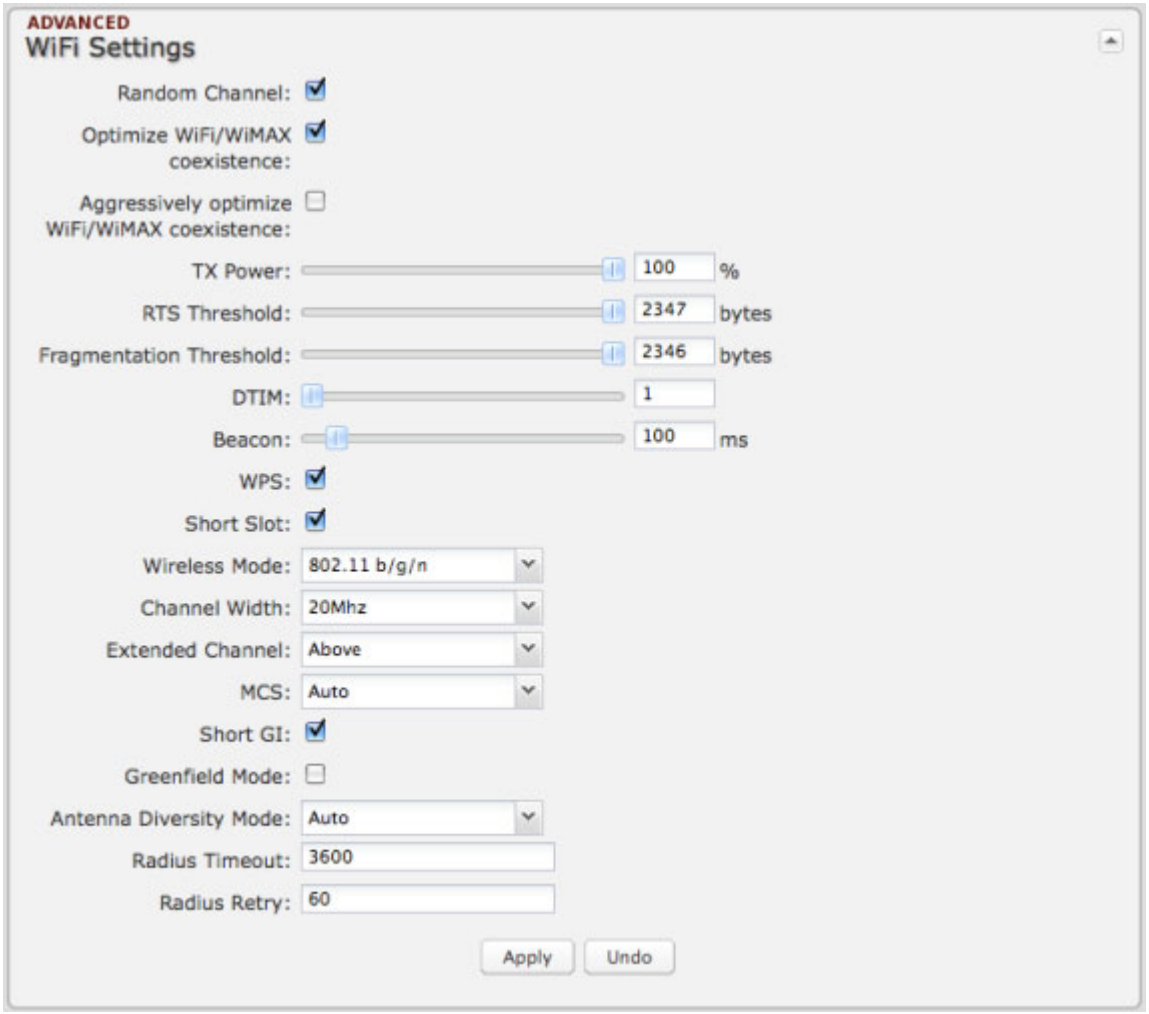
- ~~"P~~**Personal**" security modes require passwords.
- ~~"E~~**Enterprise**" security modes are linked to a RADIUS server and require RADIUS authentication: **IP**, **Port**, and **Shared Key**.
- ~~"W~~**WPA2**" (Personal or Enterprise) forces AES as the WPA Cipher.
- ~~"W~~**WPA/WPA2**" and ~~"W~~**WPA**" (Personal or Enterprise) allow AES, TKIP/AES, and TKIP.
- ~~"W~~**WEP Auto**" requires a WEP Key.
- ~~"O~~**Open**" has no password or other security measures.

NOTE: If you don't know whether you should choose Personal or Enterprise, assume Personal since you need to know RADIUS authentication for Enterprise.

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose **WPA2/AES** for security if your attached devices can support it. WEP and WPA/TKIP are obsolete and have been replaced by WPA/AES. Using those security settings will cause the WiFi to limit to 802.11g modes.

Click **Submit** to save changes.

6.7.3 WiFi Settings



Random Channel: Select to randomize the WiFi channel. This makes it less likely that the wireless signal from this router will conflict with another router in the same area.

Channel: The WiFi channel corresponds to a frequency the router uses to communicate with other devices. The range is 1 to 11, and 1, 6, and 11 do not overlap each other. If a WiMAX modem is attached, a higher number channel will increase the chance the router's WiFi and modem's WiMAX radios will conflict with each other, which may result in lower throughput. Select a channel from the dropdown list:

- 1 (2412 MHz)
- 2 (2417 MHz)
- 3 (2422 MHz)
- 4 (2427 MHz)
- 5 (2432 MHz)
- 6 (2437 MHz)
- 7 (2442 MHz)
- 8 (2447 MHz)
- 9 (2452 MHz)
- 10 (2457 MHz)
- 11 (2462 MHz)

Optimize WiFi/WiMAX coexistence: Setting this will lessen any possible conflict with WiFi in the 2.4 GHz band and an attached WiMAX modem. If a WiMAX modem is attached to the router when the WiFi is enabled, the WiFi channel and transmit power will be set to levels that optimize the performance of the WiMAX modem. If no WiMAX modem is attached, then default channel and power settings will be used even if this is selected.

Aggressively optimize WiFi/WiMAX coexistence: Selecting this will allow the router to switch WiFi channels and power levels to match changes in WiMAX modem operating frequencies. This may cause some attached WiFi clients to lose their connection. This is disabled if WiFi as WAN is enabled, as the router will need to match the WiFi channel of the host router.

TX Power: Normally the wireless transmitter operates at 100% power. In some circumstances, however, there might be a need to isolate specific frequencies to a smaller area. By reducing the power of the radio, you can prevent transmissions from reaching beyond your corporate/home office or designated wireless area.

RTS Threshold: When an excessive number of wireless packet collisions are occurring, wireless performance can be improved by using the RTS/CTS (Request to Send/Clear to Send) handshake protocol. The wireless transmitter will begin to send RTS frames (and wait for CTS) when data frame size in bytes is greater than the RTS Threshold. This setting should remain at its default value.

Fragmentation Threshold: Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage. Fragmentation will occur when frame size in bytes is greater than the Fragmentation Threshold. This setting should remain at its default value. Setting the Fragmentation value too low may result in poor performance.

DTIM: A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.

Beacon: Beacons are packets sent by a wireless router to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000 milliseconds.

WPS: WiFi Protected Setup is a method for easy and secure establishment of a wireless network. It can be used instead of passwords when connecting clients that support WPS.

Short Slot: Slot Time is the period wireless clients use in determining if the channel is free for transmission. Enabling this value allows clients that can utilize a shorter time to do so. Disabling this option forces all clients to use a longer backoff check and thus may reduce network throughput while reducing the number of transmission collisions.

Wireless Mode: Select the WiFi clients the router will be compatible with. Greater compatibility is a tradeoff with better performance. For greatest compatibility with all WiFi devices, select "802.11 b/g/n". For best performance, connect with only other 802.11n-compatible devices and select "802.11 n".

- 802.11 b
- 802.11 b/g
- 802.11 b/g/n
- 802.11 n

Channel Width: Selects whether the router uses a single 20 MHz channel to send/receive, or uses two adjacent 20 MHz channels to create a 40 MHz channel. Higher performance is possible with the 40 MHz channel. Selecting Auto is generally best. Enabling WiFi as WAN will force 20MHz only mode.

Extended Channel: When operating in 40 MHz mode the AP will use an extended channel either below or above the current channel. Optimal selection will depend on the channels of other networks in the area.

MCS: 802.11n uses multiple Modulation Coding Schemes to enable higher throughput in various environments. Since clients can dynamically change rates depending on environment selecting Auto is generally best.

Short GI: Short GI is an optimization for shortening the interval between transmissions. May be incompatible with older clients.

Greenfield Mode: Greenfield mode uses an 802.11n-only preamble to transmit packets that older wireless clients cannot interpret. Use of greenfield mode in a mixed 802.11 environment may result in degraded performance but can improve performance if all devices in the area are 802.11n compatible.

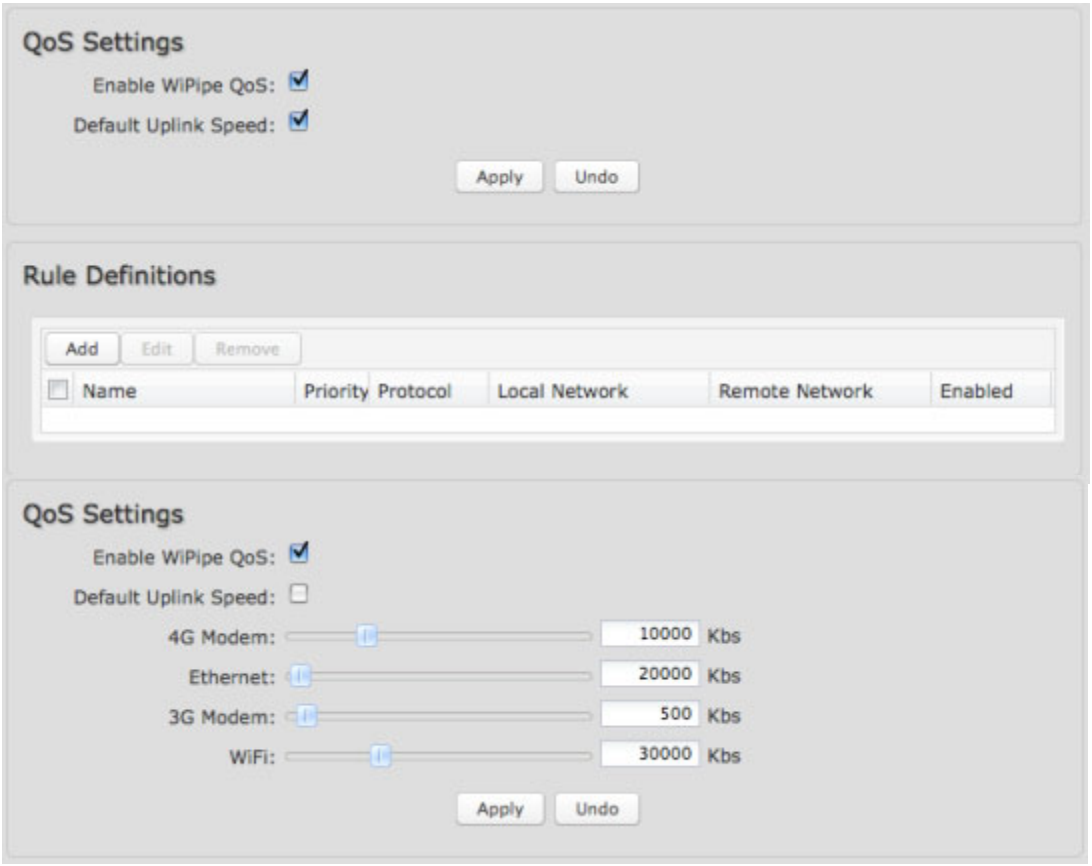
Antenna Diversity Mode: Antenna Diversity selects the optimal antenna to use for wireless reception. Automatic mode periodically checks both antennas and selects the one with best receive signal strength. Forcing a specific antenna will disable the periodic check and use the selected antenna for all wireless reception.

- Auto
- Force antenna 1
- Force antenna 2

RADIUS Timeout: (Default: 3600 seconds) When using an Enterprise security mode clients will be forced to re-authenticate with the RADIUS server at this interval in seconds. This allows administrators to revoke access so when an attached client‘s authentication expires they must re-authenticate.

RADIUS Retry: (Default: 60 seconds) When using an Enterprise security mode, if a RADIUS query fails to receive a response from the server it will delay by this interval (in seconds) before attempting another query. This helps protect the network from floods of authentication requests if the RADIUS server is temporarily unreachable.

6.8 *WiPipe QoS (Advanced Mode only)*



When WiPipe QoS (Quality of Service/Traffic Shaping) is enabled, the router will control the flow of internet traffic according to the user-defined rules. In other words, Traffic Shaping improves performance by allowing the user to prioritize applications.

Enable WiPipe QoS: Click on this box to open options for controlling internet traffic. You can control Uplink Speed values or define your own Traffic Shaping rules. When WiPipe QoS is enabled, the router restricts the flow of outbound traffic so as not to exceed the WAN uplink bandwidth.

Default Uplink Speed: By default, the Uplink Speed values are set as fast as possible. Click to deselect default values if you want to restrict the maximum uplink speed for the internet source(s) you are using (4G Modem, Ethernet, 3G Modem, and/or WiFi).

You might do this to reduce overall bandwidth use for cost reasons or to prioritize available bandwidth for download. It is recommended that you experiment with different values for your particular internet connection to yield the best results.

NOTE: Uplink speed is the speed at which data can be transferred to your ISP. You can test your uplink speed with a service such as speedtest.net.

6.8.1 Add Traffic Shaping Rule

A Traffic Shaping Rule identifies a specific message flow and assigns a priority to that flow. For most applications,

automatic classification will be adequate, and specific Traffic Shaping Rules will not be required.

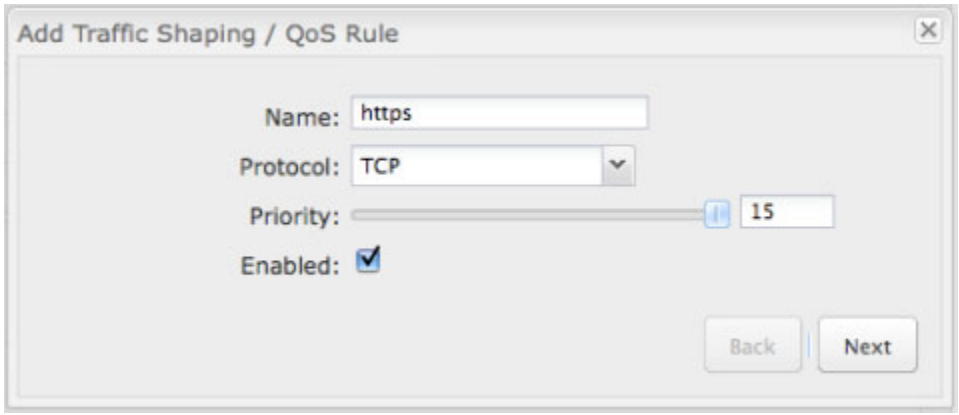
Traffic Shaping supports overlap between rules, where more than one rule can match for a specific message flow. If more than one rule matches, the rule with the highest priority will be used.

Name. Create a name for the rule that is meaningful to you.

Protocol. The protocol used by the messages: TCP, UDP, or ICMP. Select —Any" if your rule does not control a specific type of message that uses a specific protocol.

Priority. The priority of the message flow is entered here--15 receives the highest priority (most urgent) and 0 receives the lowest priority (least urgent).

Enable. Specifies whether the entry will be active or inactive.



Click **Next** to continue to the next page.

Example: You sometimes work from home, and you share bandwidth with your children. You can set a rule to prioritize your computer and a rule to reduce priority for their computer. To prioritize your computer, you might use the following settings:

- **Name:** My Computer
- **Protocol:** Any (Your computer will use all three protocols; there's no reason to restrict this rule to just one protocol)
- **Priority:** 15

To lower the priority of your children's computer, you might use these settings:

- **Name:** Kids' Computer
- **Protocol:** Any
- **Priority:** 2

The second page allows you to designate the computer(s) on the local network for which you want to adjust traffic priority.

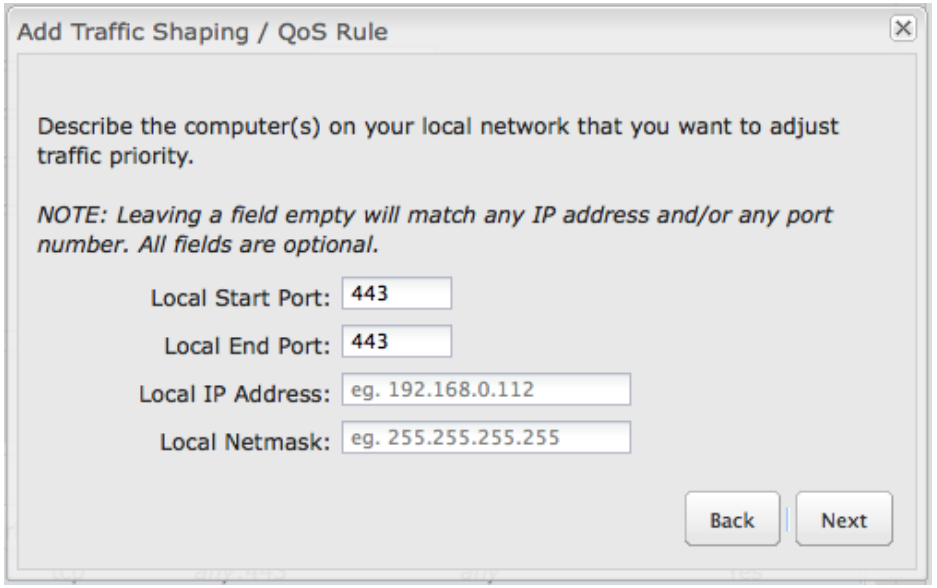
NOTE: Leaving a field empty will match any IP address and/or any port number. **All fields are optional.**

Local Start Port and **Local End Port:** The rule applies to a flow of messages whose LAN-side port number is within the range set here.

Local IP Address: The rule applies to a flow of messages with this LAN-side IP address.

Local Netmask: The rule applies to a flow of messages with this LAN-side netmask.

Example *(continued from previous page)*: To select your computer or your kids' computer, you only need to input the Local IP Address. You can ignore the other settings on this page.



The third and last page allows you to designate the network or server on the internet for which you want to shape traffic.

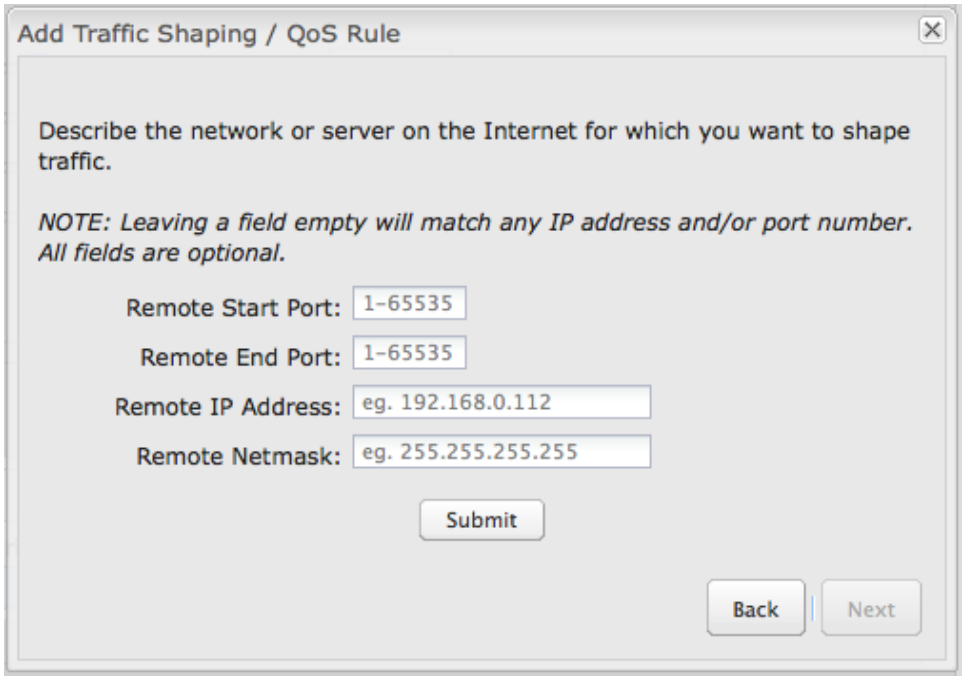
NOTE: Leaving a field empty will match any IP address and/or any port number. **All fields are optional.**

Remote Start Port and **Remote End Port:** The rule applies to a flow of messages whose WAN-side port number is within the range set here.

Remote IP Address. The rule applies to a flow of messages with this WAN-side IP address.

Remote Netmask. The rule applies to a flow of messages with this WAN-side Netmask.

Submit. Click to record the changes you have made.



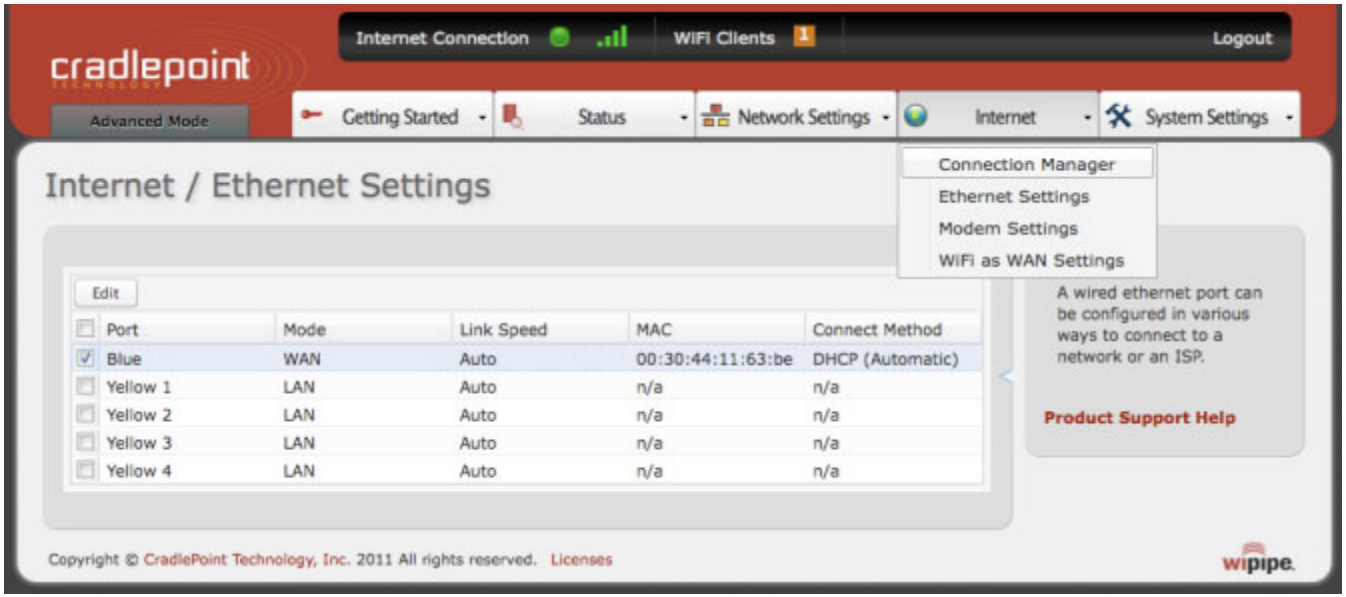
Example *(continued from previous page)*: Since the goal is simply to control which devices in your network get priority, you can ignore all of the remote settings. Leave them blank to include all possibilities.

7 INTERNET

The Internet tab provides access to 7 submenu items for managing a variety of internet connection options.

- Connection Manager
- Ethernet Settings
- Modem Settings
- **WiFi as WAN Settings**

(**WiFi as WAN Settings**: Advanced Mode only)

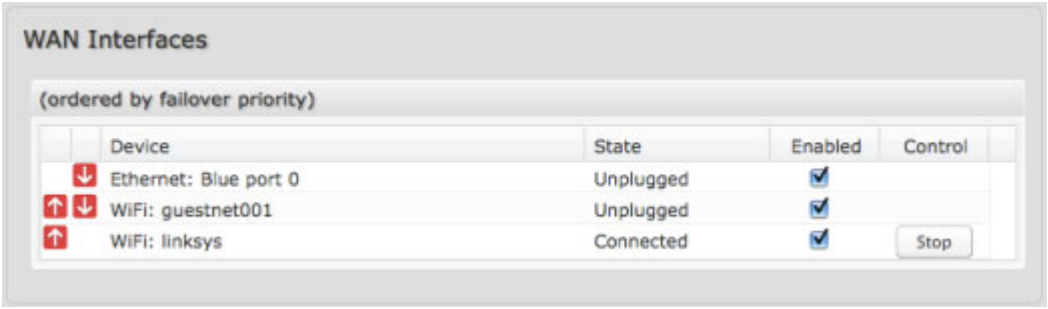


7.1 *Connection Manager*

The router can establish an uplink via the Ethernet WAN port, WiFi as WAN, or modems plugged into a modem port. If the primary WAN connection fails the router will automatically attempt to bring up a new link on another device. This feature is called failover. If Load Balance is enabled, multiple WAN devices may be plugged in and each may establish a link.

7.1.1 WAN Interfaces

This is a list of the available interfaces used to access the internet. You can enable, stop, or start devices from this section. By using the priority arrows (the arrows in the red boxes; these show if you have more than one available interface), you can set the interface the router uses by default and the order that it allows failover. To configure a specific interface, use the settings page for that type of interface (e.g. Ethernet Settings page for wired connections).



7.1.2 Failure Check (Advanced Mode Only)

If this is enabled, the router will check that the highest priority active WAN interface can get to the internet even if the WAN connection is not actively being used. If the interface goes down, the router will switch to the next highest priority interface available. If this is not selected, the router will still failover to the next highest priority interface but only after the user has attempted to get out to the internet and failed.

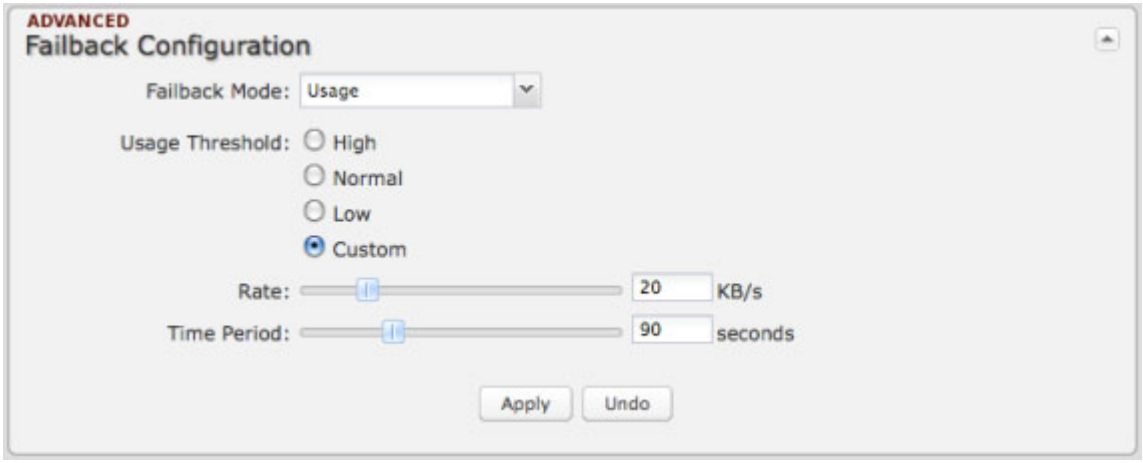
Idle Check Interval: The amount of time between each check. (Default: 30 seconds. Range: 10-3600 seconds.)

ICMP Ping Check and **Ping IP Address:** Enable and configure an IP address that the router will use to check if the WAN connection is available. For best results, select an established public IP address.

For example, you might ping Google Public DNS at 8.8.8.8 or Level 3 Communications at 4.2.2.2.

7.1.3 Failback Configuration (Advanced Mode Only)

This is used to configure failback, which is the ability to go back to a higher priority WAN interface if it regains connection to its network.



Usage: Failback based on the amount of data passed over time. Use of the active connection must be below this threshold for failback to occur. This will limit the interruption that occurs during failback.

- **High** (Rate: 80 KB/s. Time Period: 30 seconds.)
- **Normal** (Rate: 20 KB/s. Time Period: 90 seconds.)
- **Low** (Rate: 10 KB/s. Time Period: 240 seconds.)
- **Custom** (Rate range: 1-100 KB/s. Time Period range: 10-300 seconds.)

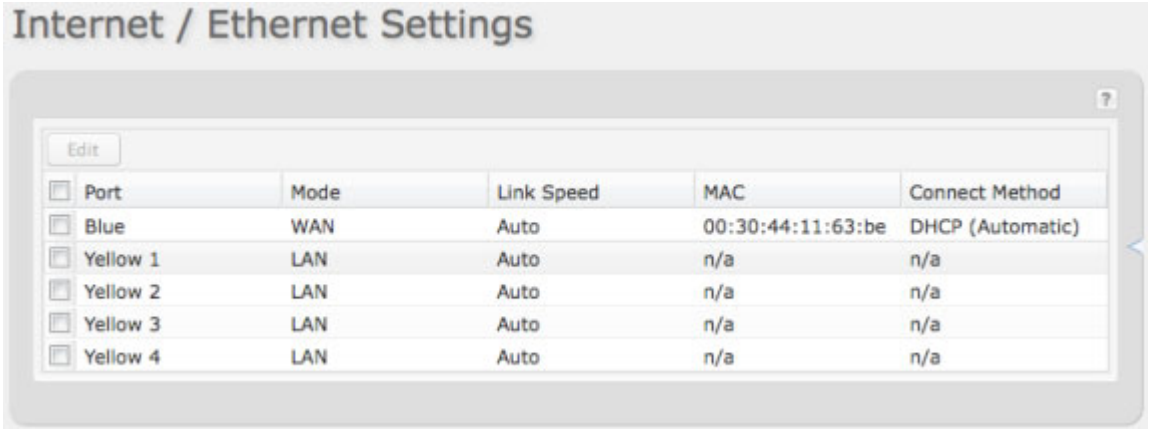
Time: Failback only after a set period of time. (Default: 90 seconds. Range: 10-300 seconds.) This ensures that the higher priority interface has remained online for a set period of time before it becomes active (in case the connection is dropping in and out, for example).

Immediate: Failback immediately whenever a higher priority interface is plugged in or when there is a priority change. Immediate failback returns you to the use of your preferred internet source more quickly which may have advantages such as reducing the cost of a failover data plan, but it may cause more interruptions in your network than **Usage** or **Time** modes.

Disabled: Deactivate failback mode.

7.2 *Ethernet Manager*

The Ethernet Manager provides controls for your router's Ethernet ports. There are five total ports: one blue WAN port and four numbered yellow LAN ports. While default settings will be sufficient in most circumstances, you have the ability to control: **Link Speed**, **MAC** addresses, and **Connect Method** for the WAN port and **Link Speed** for the LAN ports.



7.2.1 Mode

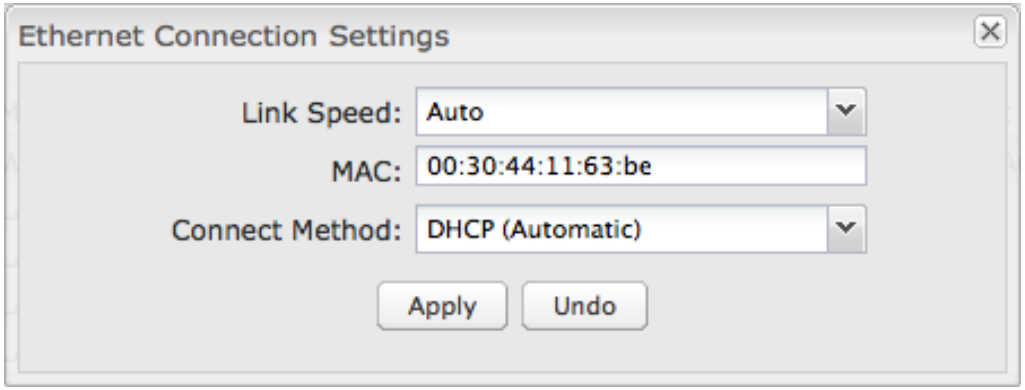
WAN or LAN. The blue port is WAN (Wide Area Network) and the four yellow ports are LAN.

- **WAN** (Wide Area Network) is used to connect to another network such as a hotel or office wired network. The WAN connection is used as a possible source of internet for the MBR95.
- **LAN** (Local Area Network) is for connecting a computer or similar device directly to the router with an Ethernet cable.

7.2.2 Link Speed

Default setting is Auto. The Auto setting is preferred in most cases.

- Auto
- 10Mbps - Half Duplex
- 10Mbps - Full Duplex
- 100Mbps - Half Duplex
- 100Mbps - Full Duplex

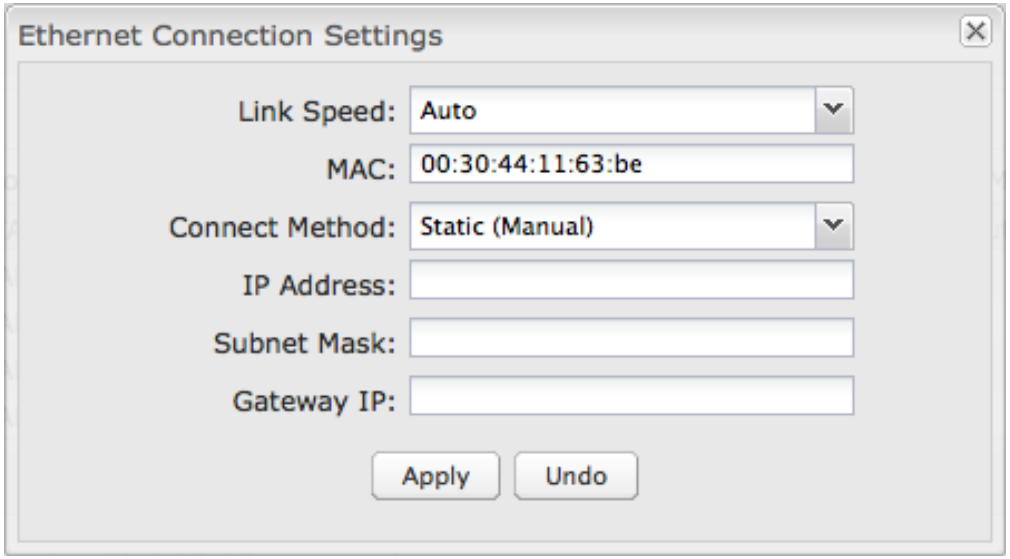


7.2.3 MAC

Only applicable in WAN mode. You have the ability to change this MAC address, but typically this is unnecessary.

7.2.4 Connect Method

Only applicable in WAN mode. Your router's Ethernet ports are automatically configured for DHCP connection. If you want to use a Static (Manual) or PPPoE connection instead, you will need to fill out additional information.



DHCP (Automatic)

Static (Manual):

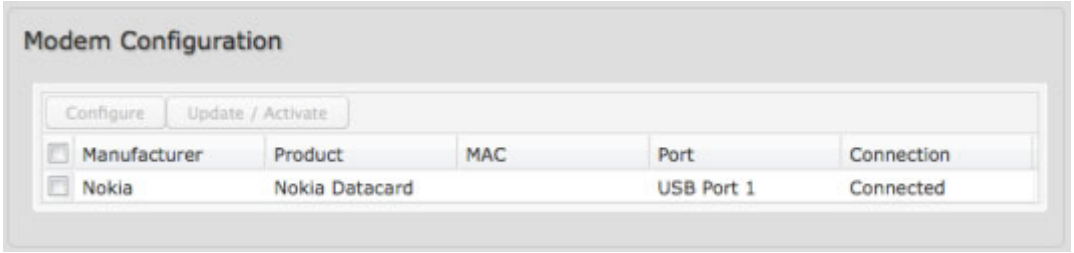
- IP Address
- Subnet Mask
- Gateway IP

PPPoE:

- Username
- Password
- Password Confirm
- Service
- Auth Type: None, PAP, CHAP

7.3 *Modem Settings*

This section shows all attached modems and allows you to change settings. If you have a 3G/4G dual-mode modem it will show both modems using the same USB port.

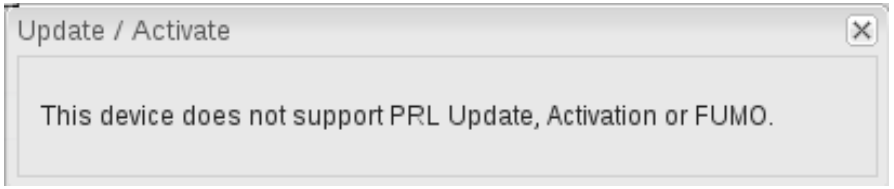


7.3.1 Update/Activate a Modem

Some 3G modems can be updated and activated while plugged into the router. Updates and activation methods vary by modem model and service provider. Possible methods are: PRL Update, Activation, and FUMO. All supported methods will be displayed when you select your modem and click "Update/Activate". If no methods are displayed for your device then you will need to update and activate your device externally.

To update or activate a modem, select the checkbox next to the device and click "Update / Activate".

The modem *does not* support Update/Activate methods: A message will state that there is no support for PRL Update, Activation, or FUMO.



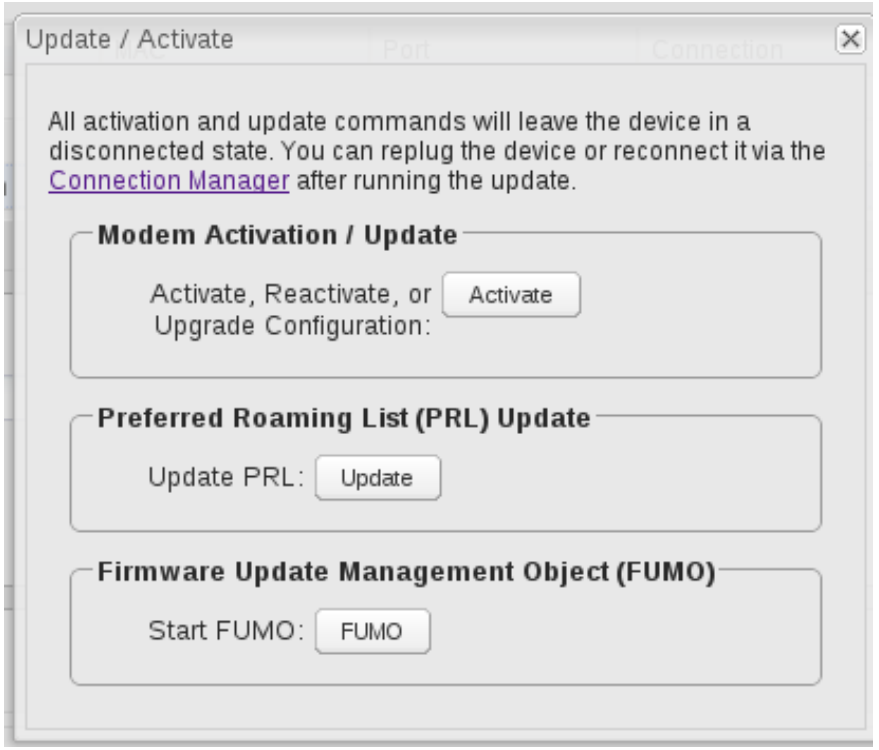
The modem supports Update/Activate methods: A message will display showing options for each supported method:

- **Modem Activation / Update:** Activate, Reactivate, or Upgrade Configuration.
- **Preferred Roaming List (PRL) Update**
- **Firmware Update Management Object (FUMO)**

Click the appropriate icon to start the process.

If the modem is connected when you start an operation the router will automatically disconnect it. The router may start another modem as a failover measure. When the operation is done the modem will go back to an idle state, at which point the router may restart it depending on failover and failback settings.

NOTE: Only one operation is supported at a time. If you try to start the *same* operation on the *same* modem twice the UI will not report failure and the request will finish normally when the original request is done. However if you try to start a *different* operation or use a *different* modem, this second request will fail without interfering with the pending operation.



Process Timeout: If the process fails an error message will display.

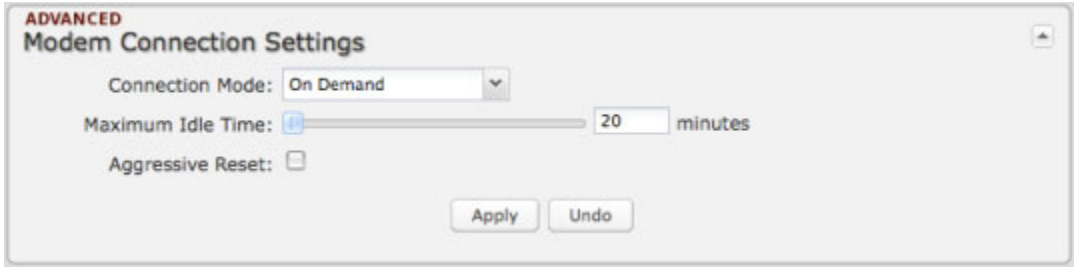
Activation has a 3-minute timeout, PRL update has a 4-minute timeout, and FUMO has a 10-minute timeout.

7.3.2 Modem Connection Settings (Advanced Mode Only)

This section changes settings that affect how all modems attempt to connect to the service provider's network.

Connection Mode: Typically modem connections are not set to remain on. The router allows you to set the type of reconnection mode.

- **Always On:** A connection to the internet is continuously maintained.
- **On Demand:** A connection to the internet is made as needed.
- **Manual:** The administrator has to navigate to the Connection Manager (**Internet → Connection Manager**) page and use the control buttons shown in the WAN Interfaces table.

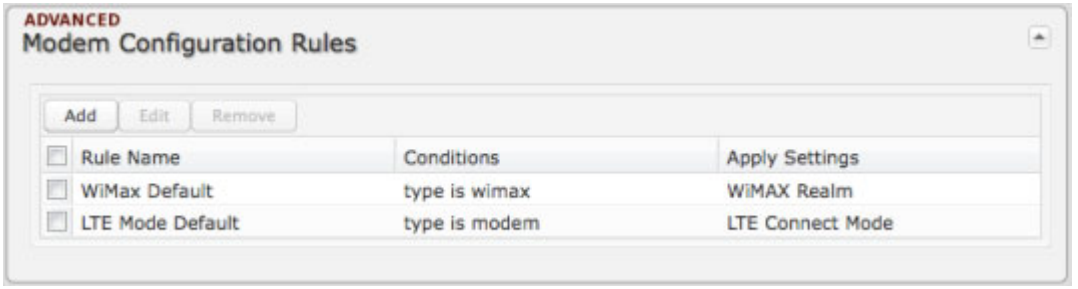


Maximum Idle Time: The interval at which the machine can be idle before the modem connection is disconnected. This setting is only valid for the "On Demand" and "Manual" connection modes.

Aggressive Reset: When Aggressive Reset is enabled the system will attempt to maintain a good modem connection. If the internet has been unreachable for a period of time a reset of the modem will occur in attempt to re-establish the connection.

7.3.3 Modem Configuration Rules (Advanced Mode Only)

This section allows you to create simple or complex rules that affect how individual modems or classes of modems (perhaps all WiMAX modems or all modems from Sierra Wireless) behave in the router.

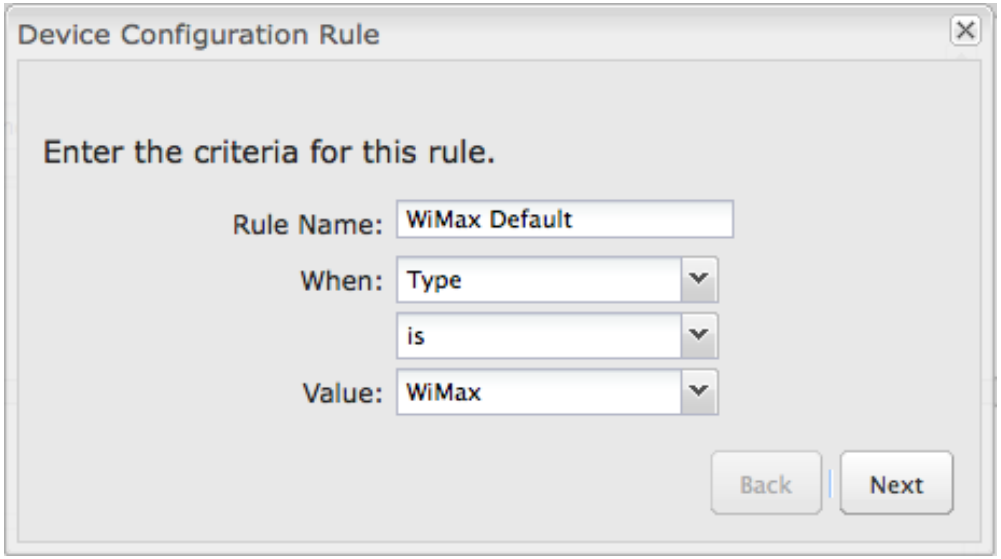


Configuration Rule: First page. Create a name for your rule and the condition for which the rule applies.

Rule Name: Create a name meaningful to you.

Select each of the following to create a condition for your rule. The condition will be of the following form:
"(When) is/is not (value)"

For example:
"Type is not WiMAX"
"Port is USB Port 1"



When:

- Port (USB Port 1, 2, 3; ExpressPort 1, 2)
- Manufacturer
- Model
- Type (WiMAX, Modem, HSPA)
- Serial Number
- MAC Address
- Unique ID

Value: If you chose Port or Type, select from the dropdown list. If you chose Manufacturer, Model, Serial Number, MAC Address, or Unique ID, you will need to manually input the information.

Configuration Rule: WiMAX Settings

WiMAX Realm:

- Clear – clearwire-wmx.net
- Rover – rover-wmx.net
- Sprint 3G/4G – sprintpcs.com
- Xohm –xohm.com
- BridgeMAXX – bridgeMAXX.com
- Time Warner Cable – mobile.rr.com
- Comcast – mob.comcast.net

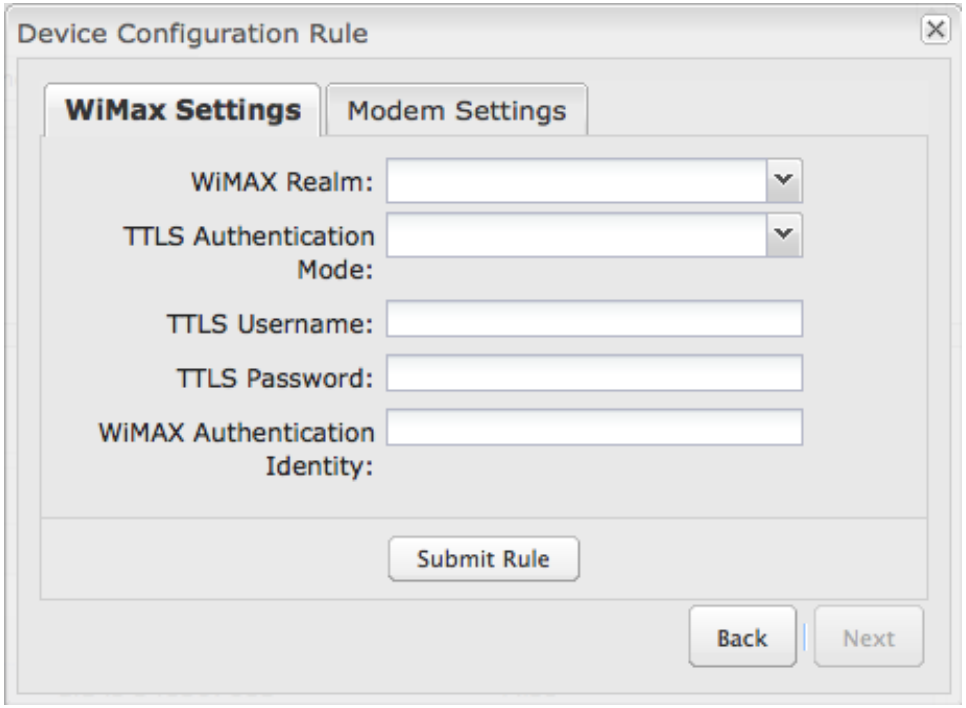
TTLS Authentication Mode: TTLS inner authentication protocol.

- MSCHAPv2/MD5
- PAP
- CHAP

TTLS Username: Username for TTLS authentication.

TTLS Password

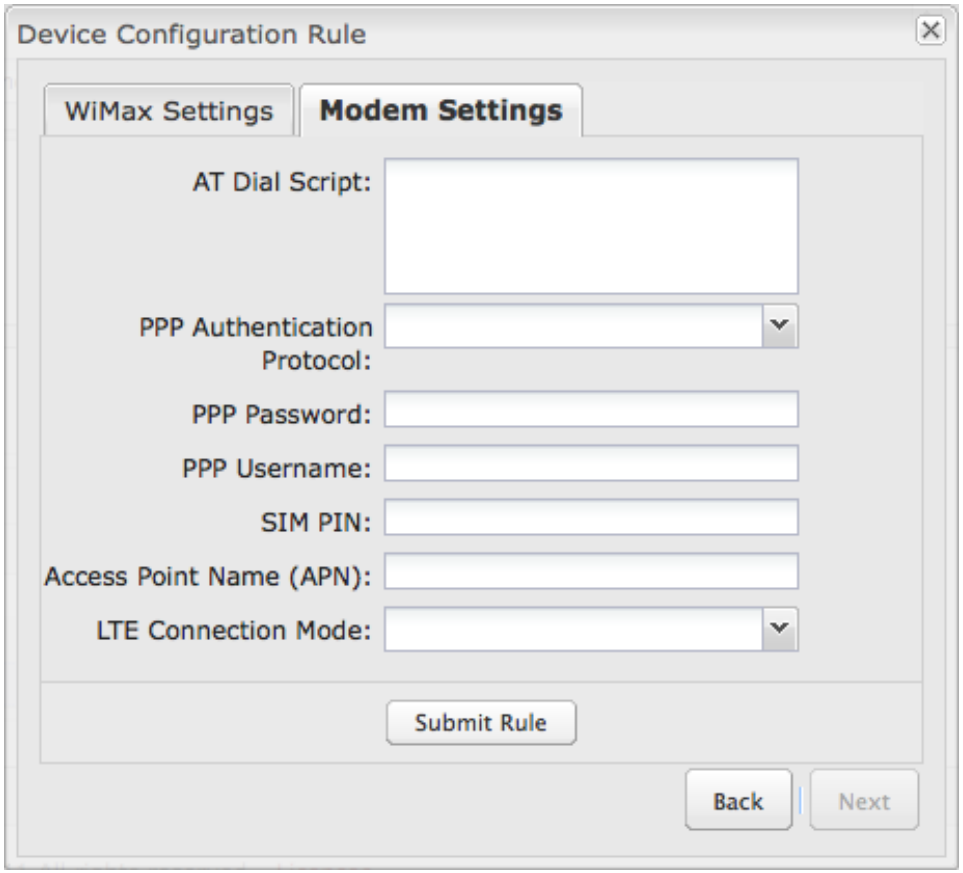
WiMAX Authentication Identity: User ID on the network. Leave this blank unless your provider tells you otherwise.



Configuration Rule: Modem Settings

AT Dial Script: Enter the AT commands to be used in establishing a network connection. Each command must be entered on a separate line. All command responses must include –OK" except the final command response, which must include —CONECT".

Example:
AT
AT+CGDCONT=2,"IP","isp.cingular"
ATCT*99***2#



PPP Authentication Protocol: Set this only if your service provider requires a specific protocol and the Auto option chooses the wrong one.

- Auto
- PAP
- CHAP

PPP Password: Password for PPP authentication.

PPP Username: Username for PPP authentication.

SIM PIN: PIN number for GSM modem with a locked SIM.

Access Point Name (APN): Some wireless carriers provide multiple Access Point Names that a modem can connect to. If you wish to specify an APN, enter it into this field. Some examples of APN are _ispcingular" and —vzwinternet.com". This APN will be set in the first profile position.

LTE Connection Mode: Specify how the LTE Multi Mode modem should connect to the network.

- Auto: Let the modem decide which network to use.
- Auto EVDO/1xRTT: Connect to CDMA, letting the modem decide which 3G network to use. Do not attempt to connect to LTE.
- Force LTE: Connect to LTE only (do not attempt to connect to CDMA/GSM).

- Force EVDO: Connect to CDMA EVDO network only.
- Force 1xRTT: Connect to CDMA 1xRTT network only.

7.4 *WiFi as WAN Settings (Advanced Mode only)*

When WiFi as WAN is enabled and configured the router will use a remote WiFi access point for internet connectivity. In other words, external WiFi—from a hotel for example—can be used as the internet source for your own private network. When enabled in the WiFi as WAN Settings page, the MBR95 will find possible WiFi sources that you can select and add. Unless the WiFi source is on an unprotected network, you will need to know the password or key.

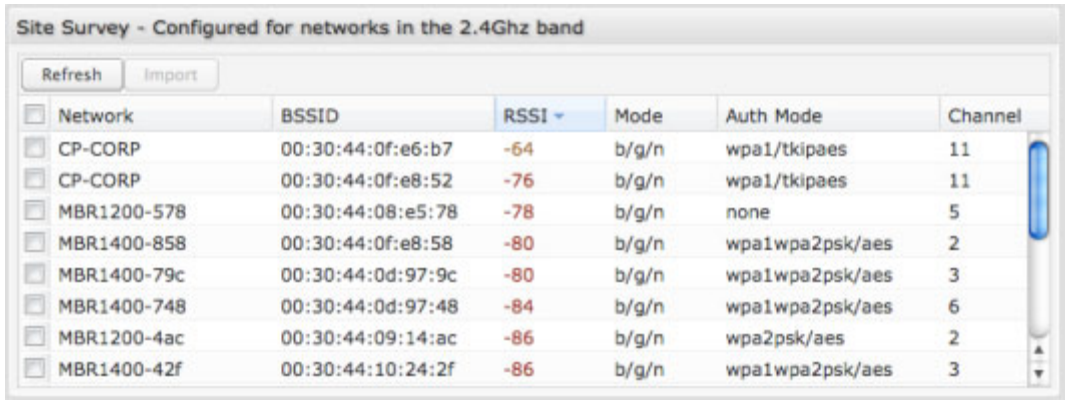
All CradlePoint routers and some other routers use the same default IP address, 192.168.0.1. If you attempt to set up WiFi as WAN and there is an —IP conflict," you need to change the IP address. The router is attempting to use the same IP address for both WAN and LAN, which is impossible. Go to **Network Settings → Local Network**. In the —LAN Settings" section you can change the IP address. For example, you might change 192.168.**0**.1 to 192.168.**1**.1.

Saved Profiles:
This is a list of WiFi networks that have already been configured as WAN sources. The router will attempt to connect to any of these access points using the password you have configured. If more than one access point is in range, then the router will connect with the highest priority network.

7.4.1 Site Survey

This is a list of WiFi networks that the router can currently find, along with information about the network such as its mode and channel. If you click on a network in the **Site Survey**, you can import it as a saved profile. You can sort the list based on any of the fields by clicking on the field name.

Click —Refresh" if a WiFi network to which you



want to connect is invisible.

Network Name (SSID): The name that is broadcast from each access point.

Network ID (BSSID): The numeric ID of the network. This parameter is required when trying to connect to a hidden network using WiFi as WAN. It is optional when connecting to a visible network.

Auth Mode: The type of encryption that is used by the network.

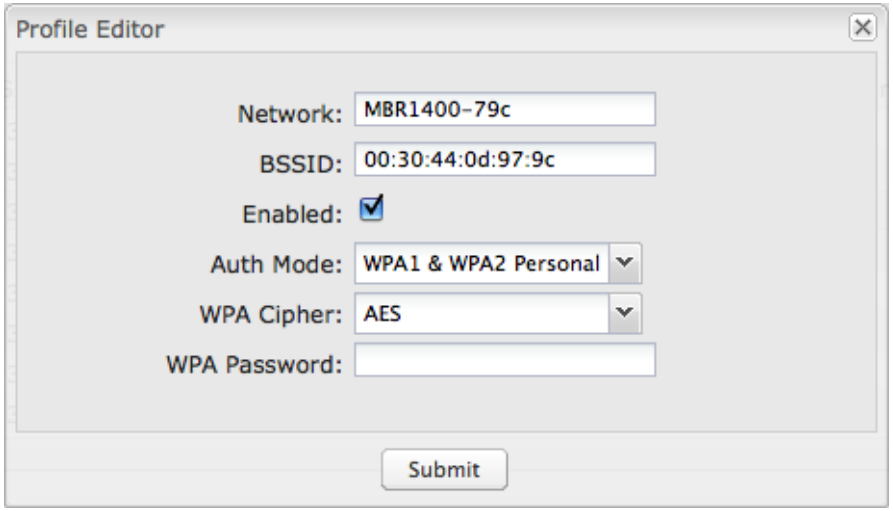
- None
- WEP Auto
- WEP Open
- WEP Shared
- WPA1 Personal
- WPA2 Personal
- WPA1 & WPA2 Personal

Channel: The channel the network is using.

7.4.2 Profile Editor

You have the option to manually add network profiles, but it is usually much easier to import them from **Site Survey**. Either click on **Add** under "**Saved Profiles**" or select a WiFi network in "**Site Survey**" and click **Import**.

If you import a network from **Site Survey**, most of the information about the network will already be completed. You need to input the password (if there is one) and then click submit to save the WiFi as WAN profile.



7.4.3 Scanning Settings (Advanced Mode Only)

Scan Interval: How often WiFi as WAN scans the environment for updates.

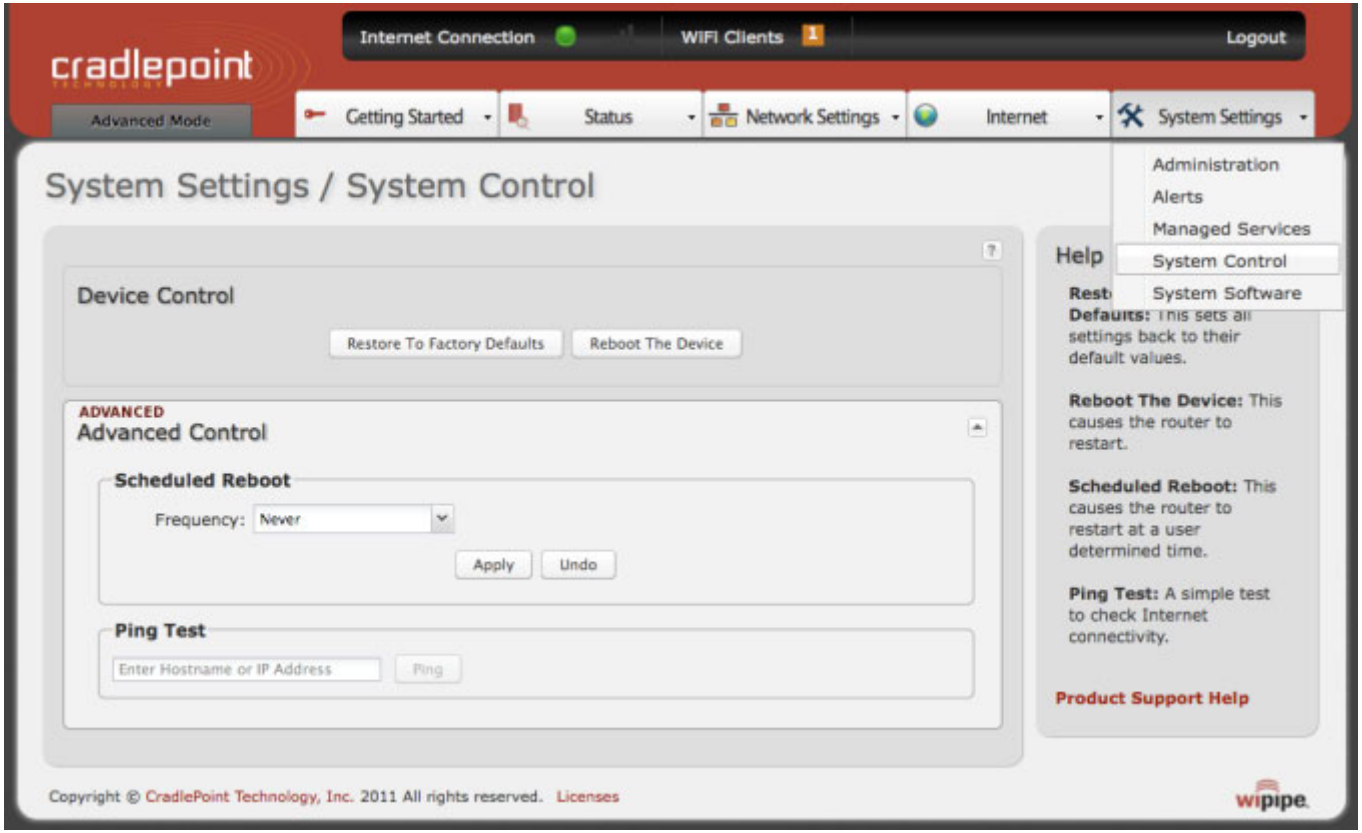
Scan While Connected: Continue to scan for WiFi as WAN profile updates when connected. Each time a scan occurs the wireless communication of the router will be temporarily interrupted. Normally this should be disabled.

8 SYSTEM SETTINGS

The System Settings tab has 6 submenu items that provide access to tools for broad administrative control of the MBR95:

- Administration
- **Alerts**
- **Managed Services**
- System Control
- System Software

(**Alerts** and **Managed Services**: Advanced Mode only)



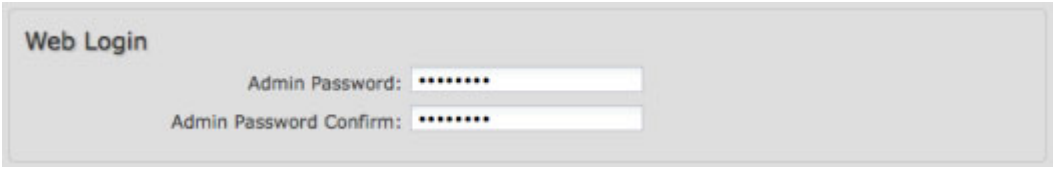
8.1 *Administration*

Select the Administration submenu item in order to control any of the following functions:

- Web Login
- Network Time Protocol
- Timezone
- Bounce Pages
- UPnP
- Remote Management

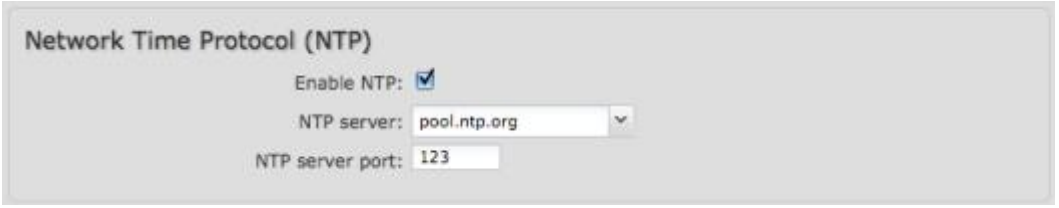
8.1.1 Web Login

This password is the administration password; this is separate from the WiFi security password. It allows a user to change router settings. This password can also be changed through the First Time Setup Wizard. The default password is found on the bottom of the MBR95.



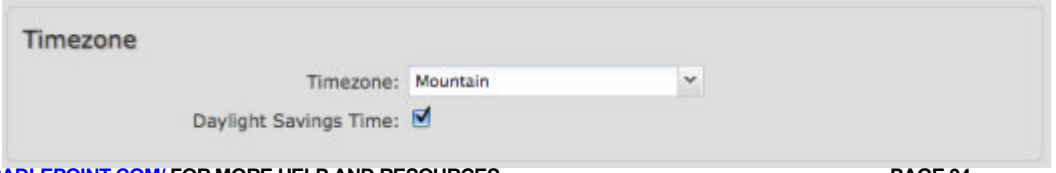
8.1.2 Network Time Protocol

Enabling NTP will tell the router to get its system time from a remote server on the internet. If you do not enable NTP then the router time will be based on when the router firmware was built, which is guaranteed to be wrong. Whenever the internet connection is re-established and once a week thereafter the router will ask the server for the current time so it can correct itself.



You then have the option of selecting an NTP server and adjusting the NTP server port. Any of the given NTP servers will be sufficient unless, for example, you need to synchronize your router‘s time with other devices in a network.

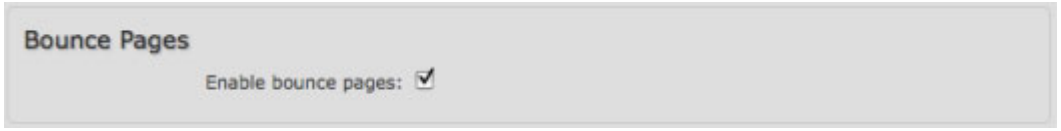
8.1.3 Timezone



This is the time zone and daylight savings setting used by the router for its own clock. This can also be controlled in the First Time Setup Wizard.

Daylight Savings Time: Select this checkbox if your location observes daylight savings time.

8.1.4 Bounce Pages



Bounce pages show up in your web browser when the router is not connected to the internet. They inform you that you are not connected and try to explain why. If you disable bounce pages then you will just get the usual browser timeout. In the normal case when the router is connected to the internet you don't see them at all.

This allows a user to disable bounce pages for cases where the router WAN link is down.

8.1.5 UPnP

Universal Plug and Play is a set of networking protocols standardized by the UPnP Forum. UPnP enables clients to determine network configuration and configure the network to allow traffic through the firewall without direct user interaction. UPnP can simplify the use of devices like game consoles and other applications that require network configuration but can also allow unprivileged users to manipulate network configuration.

8.1.6 Remote Management

Allows a user to enable incoming WAN pings or to change settings for the router from the internet using the router's internet address.

Allow WAN pings: When enabled the functionality allows an external WAN client to ping the router.

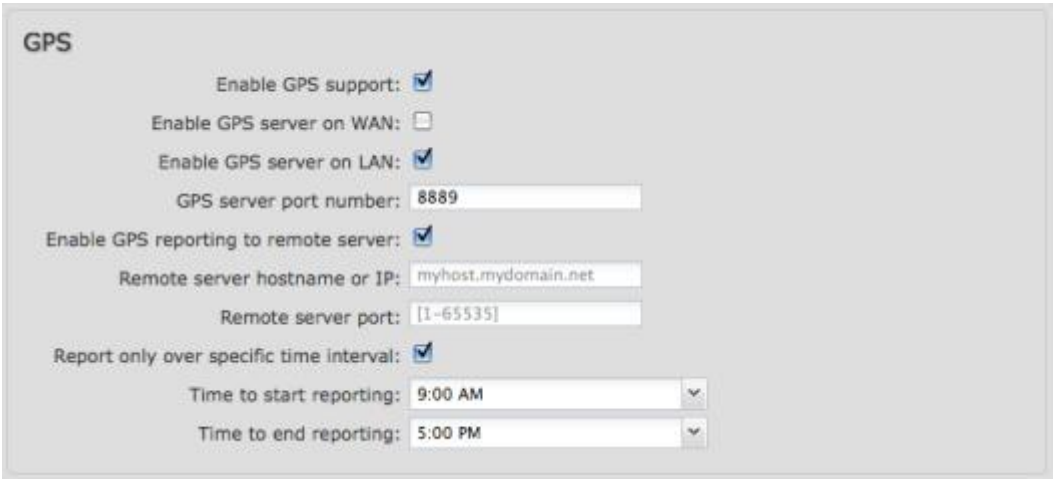
WAN Hostname: This hostname is the DNS name associated with the router's internet connection interface. If DHCP is used on the interface this hostname will be used when requesting a DHCP lease.

Allow Remote Administration: When remote administration is enabled it allows access to these administration web pages from the internet. With it disabled, you must be a client on the local network to access the administration website. For security, remote access is usually done via a non-standard http port. Additionally, encrypted connections can be required for an added level of security. Requiring a secure (**https**) connection is recommended.

8.1.7 GPS

Allows a user to configure GPS NMEA sentence reporting, available through a router-based server and/or a remote server.

NOTE: Some carriers disable GPS support in otherwise supported modems. If you encounter issues with obtaining a fix, contact your carrier and ensure that GPS is supported.

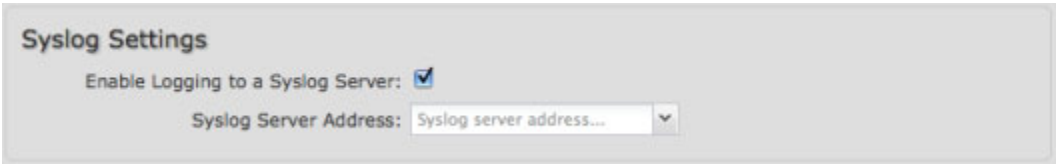


- **Enable GPS support:** Enables support for querying GPS information from supported modems.
- **Enable GPS server on WAN:** Enables a TCP server on the WAN side of the firewall which will periodically send GPS NMEA sentences to connected clients.
- **Enable GPS server on LAN:** Enables a TCP server on the LAN side of the firewall which will periodically send GPS NMEA sentences to connected clients.
    - **GPS server port number**
- **Enable GPS reporting to remote server:** Enables periodic reporting of GPS NMEA sentences to a remote server. The router will buffer NMEA data if errors are encountered or if the internet connection goes down, and send the buffered sentences when the connection is restored.
    - **Remote server hostname or IP**
    - **Remote server port**

- **Report only over specific time interval:** Restricts the NMEA sentence reporting to a remote server to a specific time interval.

8.1.8 Syslog Settings

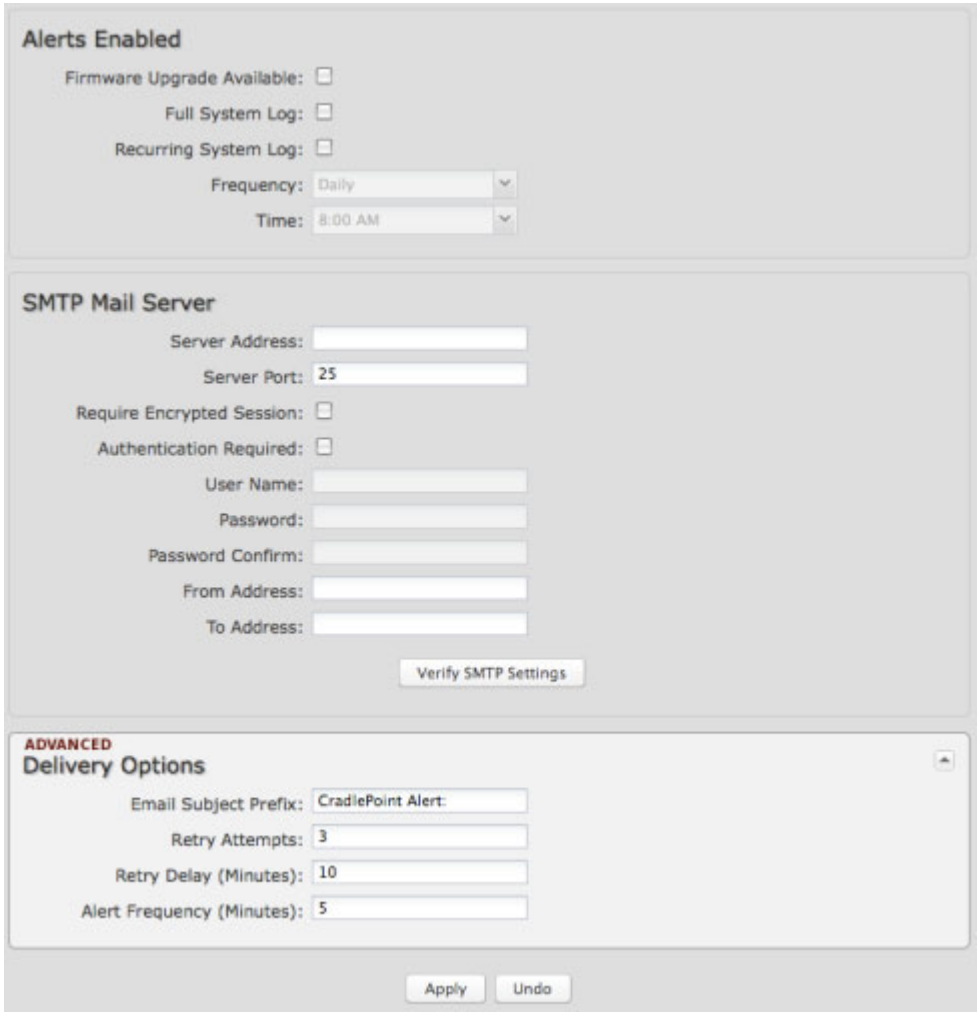
Enabling this option will send log messages to a specified Syslog server. After enabling, type the Hostname or IP address of the Syslog server.



8.2 *Alerts (Advanced Mode only)*

The Alerts submenu choice allows you to receive email notifications of specific system events. You will need to enable an SMTP email server to send alerts. Alerts can be included for the following:

- **Firmware Upgrade Available:** A firmware update is available for this device.
- **Full System Log:** The system log has filled. This alert contains the contents of the system log.
- **Recurring System Log:** The system log is sent periodically. This alert contains all of the system events since the last recurring alert. It can be scheduled for daily, weekly and monthly reports. You also choose the time you want the Alert sent.



8.2.1 SMTP Mail Server

Since the MBR95 does not have its own email server, to receive alerts you must enable an SMTP server. This is possible through most email services (Gmail, Yahoo, etc.)

Each SMTP server will have different specifications for setup, so you have to look those up separately. The following is an example using Gmail:

Server Address: smtp.gmail.com

Server Port: 587 (for TLS, or Transport Layer Security port; the MBR95 does not support SSL).

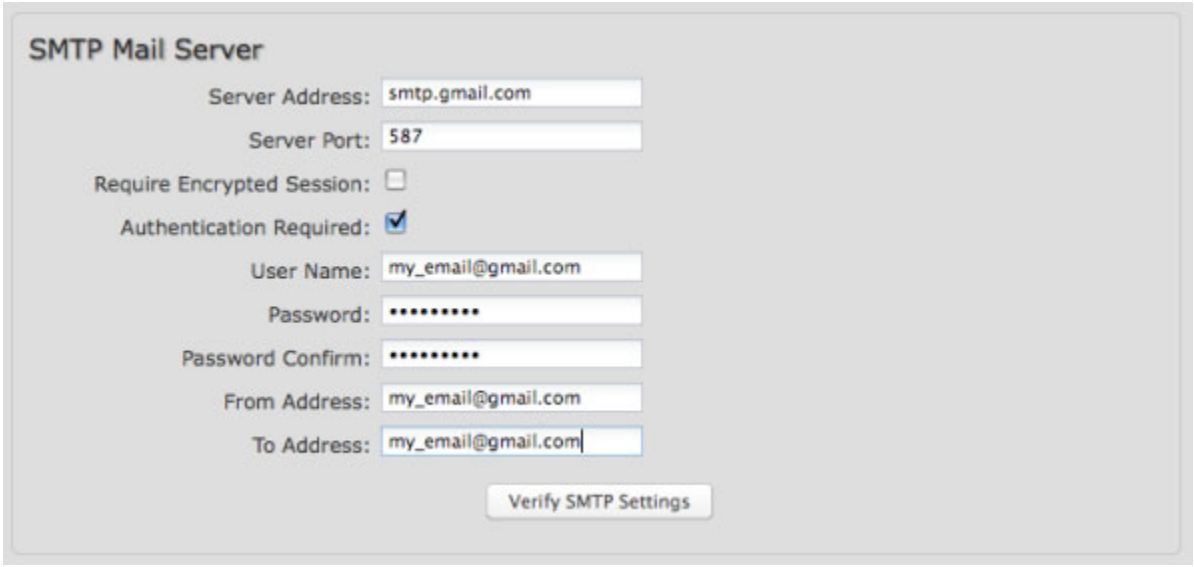
Authentication Required: For Gmail, mark this checkbox.

User Name: Your full email address

Password: Your Gmail password

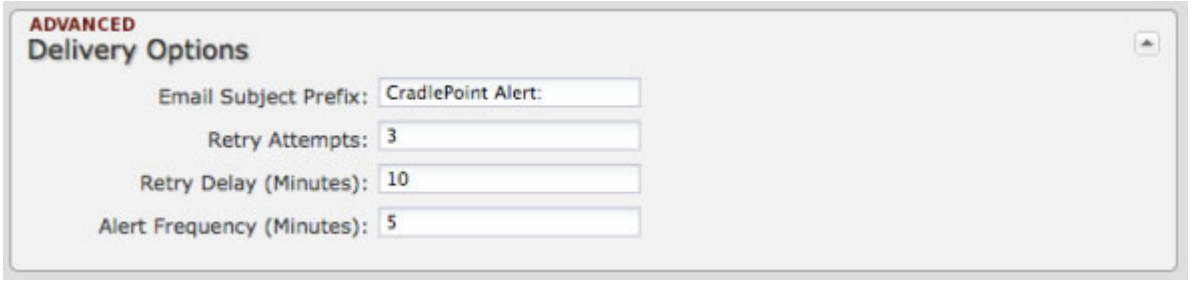
From Address: Your email address

To Address: Your email address



Once you have filled in the information for the SMTP server, click on the —Verify SMTP Settings" button. You should receive a test email at your account.

Advanced: **Delivery Options**



Email Subject Prefix: This optional string is prefixed to the alert subject. It can be customized to help you identify alerts from specific routers.

Retry Attempts: The number of attempts made to send an alert to the mail server. After the attempts are exhausted, the alert is discarded.

Retry Delay: The delay between retry attempts.

Alert Frequency: This is the maximum rate at which a specific alert will be reported. If an alert occurs more frequently, it is discarded.

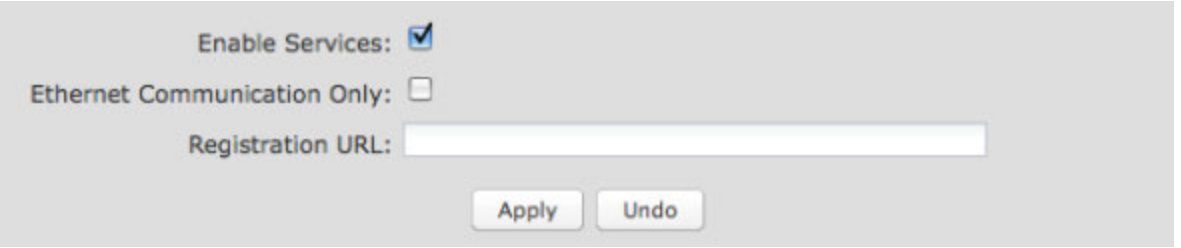
8.3 *Managed Services (Advanced Mode only) ASK YOUR CRADLEPOINT SALES REPRESENTATIVE FOR DETAILS*

Managed Services allow you to centralize your router configuration using the WiPipe Central server. WiPipe Central services must be purchased separately.

Enable Services: Enables the WiPipe Central client to contact the server.

Ethernet Communication Only: The WiPipe Central client will not start unless the WAN is Ethernet.

Registration URL: Register your router using the code provided by CradlePoint when you purchase WiPipe Central.

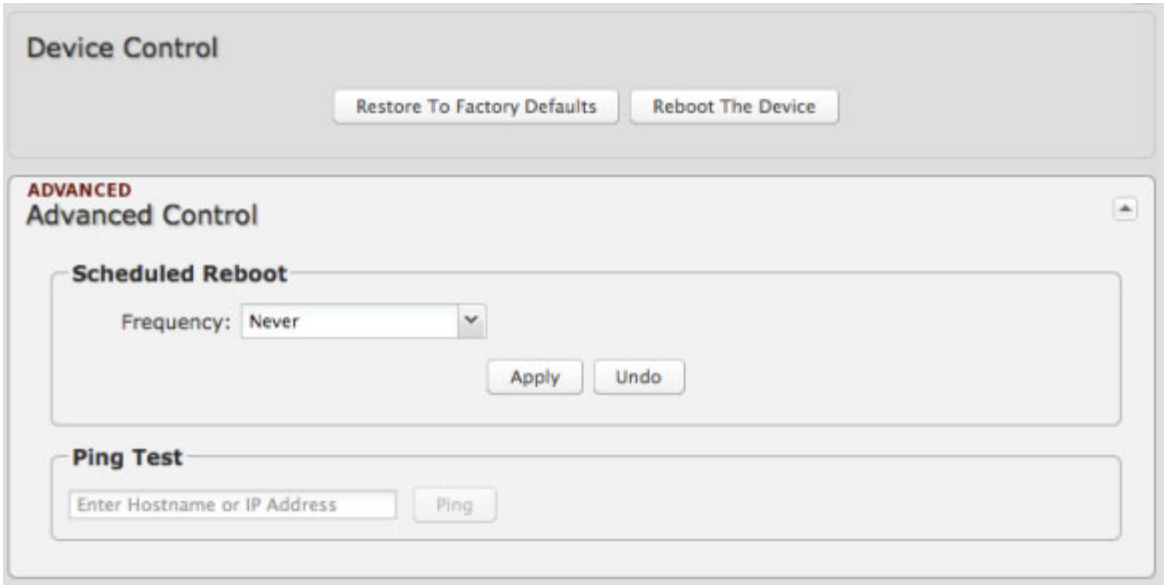


8.4 *System Control*

Restore to Factory Defaults: This changes all settings back to their default values.

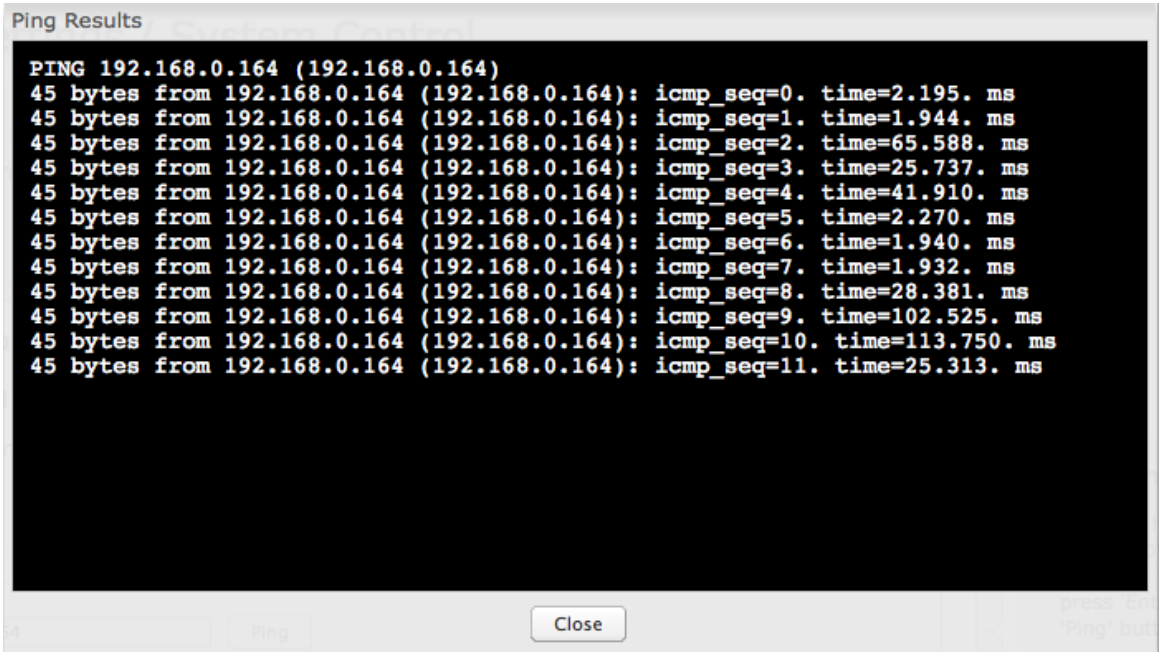
Reboot The Device: This causes the router to restart.

Advanced: Scheduled Reboot and Ping Test



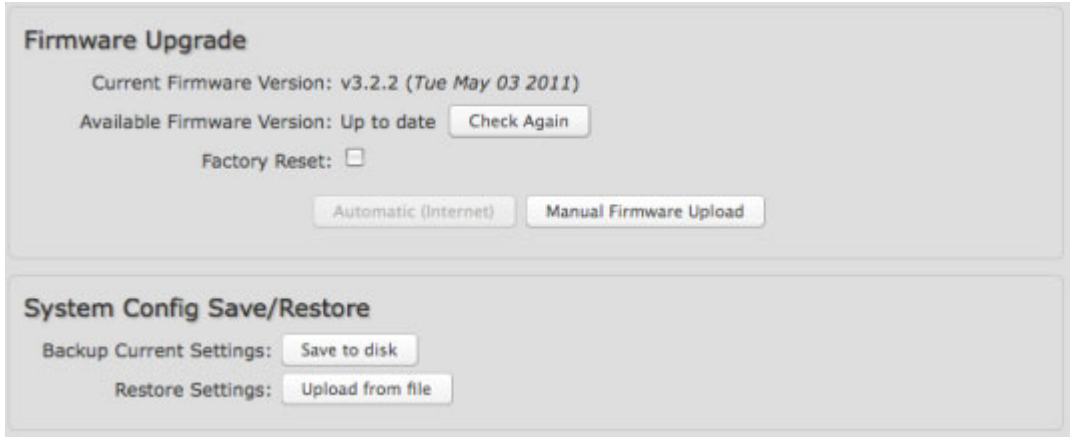
Scheduled Reboot: This causes the router to restart at a user-determined time.

Ping Test: A simple test to check internet connectivity. Type the Hostname or IP address of the computer you want to ping and press 'Enter' or click the 'Ping' button.



8.5 *System Software*

Firmware Upgrade: This allows the administrator to load new firmware onto the router to add new features or fix defects. If you are happy with the operation of the router, you may not want to upgrade just because a new version is available. Check the firmware release notes for information to decide if you should upgrade or not.



Automatic (Internet): Have the router download the file and perform the upgrade with no user interaction.

Manual Firmware Upload: Upload the router firmware from an attached computer.

Factory Reset: Set default settings to match the new firmware. This is safest, as settings may have changed. You should back up your current settings and restore them after the new firmware is loaded.

Backup Current Settings: Save your current settings to a file on a computer.

Restore Settings: Restore your previous settings from a file on a computer.

9 GLOSSARY

802.11

A family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE).

Access Control List

ACL. This is a database of network devices that are allowed to access resources on the network.

Access Point

AP. Device that allows wireless clients to connect to it and access the network.

ActiveX

A Microsoft specification for the interaction of software components.

Ad-hoc network

Peer-to-Peer network between wireless clients.

Address Resolution Protocol

ARP. Used to map MAC addresses to IP addresses so that conversions can be made in both directions.

ADSL

Asymmetric Digital Subscriber Line.

Advanced Encryption Standard

AES. Government encryption standard.

Alphanumeric

Characters A-Z and 0-9.

Antenna

Used to transmit and receive RF signals.

AppleTalk

A set of Local Area Network protocols developed by Apple for their computer systems.

AppleTalk Address Resolution Protocol

AARP. Used to map the MAC addresses of Apple computers to their AppleTalk network addresses, so that conversions can be made in both directions.

Application layer

7th Layer of the OSI model. Provides services to applications to ensure that they can communicate properly with other applications on a network.

ASCII

American Standard Code for Information Interchange. This system of characters is most commonly used for text files.

Attenuation

The loss in strength of digital and analog signals. The loss is greater when the signal is being transmitted over long distances.

Authentication

To provide credentials, like a Password, in order to verify that the person or device is really who they are claiming to be.

Automatic Private IP Addressing

APIPA. An IP address that a Windows computer will assign itself when it is configured to obtain an IP address automatically but no DHCP server is available on the network.

Backward Compatible

The ability for new devices to communicate and interact with older legacy devices to guarantee interoperability.

Bandwidth

The maximum amount of bytes or bits per second that can be transmitted to and from a network device.

Basic Input/Output System

BIOS. A program that the processor of a computer uses to startup the system once it is turned on.

Baud

Data transmission speed.

Beacon

A data frame by which one of the stations in a WiFi network periodically broadcasts network control data to other wireless stations.

Bit rate

The amount of bits that pass in given amount of time.

Bit/sec

Bits per second.

BOOTP

Bootstrap Protocol. Allows for computers to be booted up and given an IP address with no user intervention.

Bottleneck

A time during processes when something causes the process to slowdown or stop all together.

Broadband

A wide band of frequencies available for transmitting data.

Broadcast

Transmitting data in all directions at once.

Browser

A program that allows you to access resources on the web and provides them to you graphically.

Cable modem

A device that allows you to connect a computer up to a coaxial cable and receive internet access from your Cable provider.

CardBus

A newer version of the PC Card or PCMCIA interface. It supports a 32- bit data path, DMA, and consumes less voltage.

CAT 5

Category 5. Used for 10/100 Mbps or 1Gbps Ethernet connections.

Client

A program or user that requests data from a server.

Collision

When do two devices on the same Ethernet network try and transmit data at the exact same time.

Cookie

Information that is stored on the hard drive of your computer that holds your preferences to the site that gave your computer the cookie.

Data

Information that has been translated into binary so that it can be processed or moved to another device.

Data Encryption Standard

Uses a randomly selected 56-bit key that must be known by both the sender and the receiver when information is exchanged.

Data-Link layer

The second layer of the OSI model. Controls the movement of data on the physical link of a network.

Database

Organizes information so that it can be managed updated, as well as easily accessed by users or applications.

DB-25

A 25-pin male connector for attaching External modems or RS-232 serial devices.

DB-9

A 9-pin connector for RS-232 connections

dBd

Decibels related to dipole antenna.

dBi

Decibels relative to isotropic radiator.

dBm

Decibels relative to one milliwatt.

Decrypt

To unscramble an encrypted message back into plain text.

Default

A predetermined value or setting that is used by a program when no user input has been entered for this value or setting.

Demilitarized zone

DMZ: A single computer or group of computers that can be accessed by both users on the internet as well as users on the Local Network, but that is not protected by the same security as the Local Network.

DHCP

Dynamic Host Configuration Protocol: Used to automatically assign IP addresses from a predefined pool of addresses to computers or devices that request them.

Digital certificate

An electronic method of providing credentials to a server in order to have access to it or a network.

Direct Sequence Spread Spectrum

DSSS: Modulation technique used by 802.11b wireless devices.

DMZ

—Demilitarized Zone". A computer that logically sits in a —no-mans-land" between the LAN and the WAN. The DMZ computer trades some of the protection of the router's security mechanisms for the convenience of being directly addressable from the internet.

DNS

Domain Name System: Translates Domain Names to IP addresses.

Domain name

A name that is associated with an IP address.

Download

To send a request from one computer to another and have the file transmitted back to the requesting computer.

DSL

Digital Subscriber Line. High bandwidth internet connection over telephone lines.

Duplex

Sending and Receiving data transmissions at the same time.

Dynamic DNS service

Dynamic DNS is provided by companies to allow users with Dynamic IP addresses to obtain a Domain Name that will always be linked to their changing IP address. The IP address is updated by either client software running on a computer or by a router that supports Dynamic DNS, whenever the IP address changes.

Dynamic IP address

IP address that is assigned by a DHCP server and that may change. Cable internet providers usually use this method to assign IP addresses to their customers.

EAP

Extensible Authentication Protocol.

Email

Electronic Mail is a computer-stored message that is transmitted over the internet.

Encryption

Converting data into cyphertext so that it cannot be easily read.

Ethernet

The most widely used technology for Local Area Networks.

Fiber optic

A way of sending data through light impulses over glass or plastic wire or fiber.

File server

A computer on a network that stores data so that the other computers on the network can all access it.

File sharing

Allowing data from computers on a network to be accessed by other computers on the network with different levels of access rights.

Firewall

A device that protects resources of the Local Area Network from unauthorized users outside of the local network.

Firmware

Programming that is inserted into a hardware device that tells it how to function.

Fragmentation

Breaking up data into smaller pieces to make it easier to store.

FTP

File Transfer Protocol. Easiest way to transfer files between computers on the internet.

Full-duplex

Sending and Receiving data at the same time.

Gain

The amount an amplifier boosts the wireless signal.

Gateway

A device that connects your network to another, like the internet.

Gbps

Gigabits per second.

Gigabit Ethernet

Transmission technology that provides a data rate of 1 billion bits per second.

GUI

Graphical user interface.

H.323

A standard that provides consistency of voice and video transmissions and compatibility for video conferencing devices.

Half-duplex

Data cannot be transmitted and received at the same time.

Hashing

Transforming a string of characters into a shorter string with a predefined length.

Hexadecimal

Characters 0-9 and A-F.

Hop

The action of data packets being transmitted from one router to another.

Host

Computer on a network.

HTTP

Hypertext Transfer Protocol is used to transfer files from HTTP servers (web servers) to HTTP clients (web browsers).

HTTPS

HTTP over SSL is used to encrypt and decrypt HTTP transmissions.

Hub

A networking device that connects multiple devices together.

ICMP

Internet Control Message Protocol.

IEEE

Institute of Electrical and Electronics Engineers.

IGMP

Internet Group Management Protocol is used to make sure that computers can report their multicast group membership to adjacent routers.

IIS

Internet Information Server is a WEB server and FTP server provided by Microsoft.

IKE

Internet Key Exchange is used to ensure security for VPN connections.

Infrastructure

In terms of a wireless network, this is when wireless clients use an access point to gain access to the network.

Internet

A system of worldwide networks that use TCP/IP to allow for resources to be accessed from computers around the world.

Internet Explorer

A World Wide Web browser created and provided by Microsoft.

Internet Protocol

The method of transferring data from one computer to another on the internet.

Internet Protocol Security

IPsec provides security at the packet processing layer of network communication.

Internet Service Provider

An ISP provides access to the internet to individuals or companies.

Intranet

A private network.

Intrusion Detection

A type of security that scans a network to detect attacks coming from inside and outside of the network.

IP

Internet Protocol.

IP address

A 32-bit number, when talking about Internet Protocol Version 4, that identifies each computer that transmits data on the internet or on an intranet.

IPsec

Internet Protocol Security.

IPX

Internetwork Packet Exchange is a networking protocol developed by Novell to enable their Netware clients and servers to communicate.

ISP

Internet Service Provider.

Java

A programming language used to create programs and applets for web pages.

Kbps

Kilobits per second.

Kbyte

Kilobyte.

L2TP

Layer 2 Tunneling Protocol.

LAN

Local Area Network.

Latency

The amount of time that it takes a packet to get from the one point to another on a network. Also referred to as delay.

LED

Light Emitting Diode.

Legacy

Older devices or technology.

Local Area Network

LAN. A group of computers in a building that usually access files from a server.

LPR/LPD

—Line Printer Requestor”/”Line Printer Daemon”. A TCP/IP protocol for transmitting streams of printer data.

MAC Address

A unique hardware ID assigned to every Ethernet adapter by the manufacturer.

Mbps

Megabits per second.

MDI

Medium Dependent Interface is an Ethernet port for a connection to a straight-through cable.

MDIX

Medium Dependent Interface Crossover is an Ethernet port for a connection to a crossover cable.

MIB

Management Information Base is a set of objects that can be managed by using SNMP.

Modem

A device that modulates digital signals from a computer to an analog signal in order to transmit the signal over phone lines. It also demodulates the analog signals coming from the phone lines to digital signals for your computer.

MPPE

Microsoft Point-to-Point Encryption is used to secure data transmissions over PPTP connections.

MTU

Maximum Transmission Unit is the largest packet that can be transmitted on a packet-based network like the internet.

Multicast

Sending data from one device to many devices on a network.

NAT

Network Address Translation allows many private IP addresses to connect to the internet, or another network, through one IP address.

NetBEUI

NetBIOS Extended User Interface is a Local Area Network communication protocol. This is an updated version of NetBIOS.

NetBIOS

Network Basic Input/Output System.

Netmask

Determines what portion of an IP address designates the Network and which part designates the Host.

Network Interface Card

NIC. A card installed in a computer or built onto the motherboard that allows the computer to connect to a network.

Network Layer

The third layer of the OSI model which handles the routing of traffic on a network.

Network Time Protocol

Used to synchronize the time of all the computers in a network.

NIC

Network Interface Card.

NTP

Network Time Protocol.

OFDM

Orthogonal Frequency-Division Multiplexing is the modulation technique for both 802.11a and 802.11g.

OSI

Open Systems Interconnection is the reference model for how data should travel between two devices on a network.

OSPF

Open Shortest Path First is a routing protocol that is used more than RIP in larger scale networks because only changes to the routing table are sent to all the other routers in the network as opposed to sending the entire routing table at a regular interval, which is how RIP functions.

Password

A sequence of characters that is used to authenticate requests to resources on a network.

Personal Area Network

The interconnection of networking devices within a range of 10 meters.

Physical layer

The first layer of the OSI model. Provides the hardware means of transmitting electrical signals on a data carrier.

Ping

A utility program that verifies that a given internet address exists and can receive messages. The utility sends a control packet to the given address and waits for a response.

PoE

Power over Ethernet is the means of transmitting electricity over the unused pairs in a category 5 Ethernet cable.

POP3

Post Office Protocol 3 is used for receiving email.

Port

A logical channel endpoint in a network. A computer might have only one physical channel (its Ethernet

channel) but can have multiple ports (logical channels) each identified by a number.

PPP

Point-to-Point Protocol is used for two computers to communicate with each over a serial interface, like a phone line.

PPPoE

Point-to-Point Protocol over Ethernet is used to connect multiple computers to a remote server over Ethernet.

PPTP

Point-to-Point Tunneling Protocol is used for creating VPN tunnels over the internet between two networks.

Preamble

Used to synchronize communication timing between devices on a network.

QoS

Quality of Service.

RADIUS

Remote Authentication Dial-In User Service allows for remote users to dial into a central server and be authenticated in order to access resources on a network.

Reboot

To restart a computer and reload it‘s operating software or firmware from nonvolatile storage.

Rendezvous

Apple‘s version of UPnP, which allows for devices on a network to discover each other and be connected without the need to configure any settings.

Repeater

Retransmits the signal of an access point in order to extend its coverage.

RIP

Routing Information Protocol is used to synchronize the routing table of all the routers on a network.

RJ-11

The most commonly used connection method for telephones.

RJ-45

The most commonly used connection method for Ethernet.

RS-232C

The interface for serial communication between computers and other related devices.

RSA

Algorithm used for encryption and authentication.

Server

A computer on a network that provides services and resources to other computers on the network.

Session key

An encryption and decryption key that is generated for every communication session between two computers.

Session layer

The fifth layer of the OSI model which coordinates the connection and communication between applications on both ends.

Simple Mail Transfer Protocol

Used for sending and receiving email.

Simple Network Management Protocol

Governs the management and monitoring of network devices.

SIP

Session Initiation Protocol. A standard protocol for initiating a user session that involves multimedia content, such as voice or chat.

SMTP

Simple Mail Transfer Protocol.

SNMP

Simple Network Management Protocol.

SOHO

Small Office/Home Office.

SPI

Stateful Packet Inspection.

SSH

Secure Shell is a command line interface that allows for secure connections to remote computers.

SSID

Service Set Identifier is a name for a wireless network.

Stateful Packet Inspection

A feature of a firewall that monitors outgoing and incoming traffic to make sure that only valid responses to outgoing requests are allowed to pass though the firewall.

Subnet mask

Determines what portion of an IP address designates the Network and which part designates the Host.

Syslog

System Logger -- a distributed logging interface for collecting in one place the logs from different sources. Originally written for UNIX, it is now available for other operating systems, including Windows.

TCP

Transmission Control Protocol.

TCP Raw

A TCP/IP protocol for transmitting streams of printer data.

TCP/IP

Transmission Control Protocol/Internet Protocol.

TFTP

Trivial File Transfer Protocol is a utility used for transferring files that is simpler to use than FTP but with less features.

Throughput

The amount of data that can be transferred in a given time period.

Traceroute

A utility displays the routes between you computer and specific destination.

UDP

User Datagram Protocol.

Unicast

Communication between a single sender and receiver.

Universal Plug and Play

UPnP. A standard that allows network devices to discover each other and configure themselves to be a part of the network.

Update

To install a more recent version of a software or firmware product.

Upgrade

To install a more recent version of a software or firmware product.

Upload

To send a request from one computer to another and have a file transmitted from the requesting computer to the other.

UPnP

Universal Plug and Play.

URL

Uniform Resource Locator is a unique address for files accessible on the internet.

USB

Universal Serial Bus.

UTP

Unshielded Twisted Pair.

Virtual Private Network

VPN: A secure tunnel over the internet to connect remote offices or users to their company‘s network.

VLAN

Virtual LAN.

Voice over IP

Sending voice information over the internet as opposed to the PSTN

VoIP

Voice over IP.

Wake on LAN

Allows you to power up a computer through its Network Interface Card.

WAN

Wide Area Network.

WCN

Windows Connect Now. A Microsoft method for configuring and bootstrapping wireless networking hardware (access points) and wireless clients, including PCs and other devices.

WDS

Wireless Distribution System. A system that enables the interconnection of access points wirelessly.

Web browser

A utility that allows you to view content and interact with all of the information on the World Wide Web.

WEP

Wired Equivalent Privacy is security for wireless networks that is supposed to be comparable to that of a wired network.

WiFi

Wireless Fidelity. Used to describe any of the 802.11 wireless networking specifications.

WiFi Protected Access

An updated version of security for wireless networks that provides authentication as well as encryption.

Wide Area Network

The larger network that your LAN is connected to, which may be the internet itself, or a regional or corporate network.

Wireless (WiFi) LAN

Connecting to a Local Area Network over one of the 802.11 wireless standards.

Wireless ISP

WISP. A company that provides a broadband internet connection over a wireless connection.

WISP

Wireless Internet Service Provider.

WLAN

Wireless Local Area Network.

WPA

WiFi Protected Access. A WiFi security enhancement that provides improved data encryption, relative to WEP.

xDSL

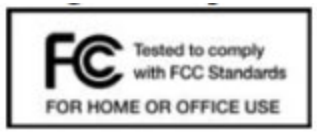
A generic term for the family of digital subscriber line (DSL) technologies, such as ADSL, HDSL, RADSL, and SDSL.

Yagi antenna

A directional antenna used to concentrate wireless signals on a specific location.

10 APPENDIX

10.1 *Regulatory Information*



This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. This device must accept any interference received, including interference that may cause undesired operation. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

- *Reorient or relocate the receiving antenna.*
- *Increase the separation between the equipment and receiver.*
- *Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.*
- *Consult the dealer or an experienced radio or television technician for help.*

Changes or modifications not expressly approved by CradlePoint, Inc. could void the user‘s authority to operate the product.

Radio Frequency Interference Requirement - Canada

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

10.2 *Warranty Information*

CradlePoint, Inc. warrants this product against defects in materials and workmanship to the original purchases (or the first purchaser in the case of resale by an authorized distributor) for a period of one (1) year from the date of shipment. This warranty is limited to a repair or replacement of the product, at CradlePoint‘s discretion.

Within thirty (30) days of receipt should the product fail for any reason other than damage due to customer negligence, purchaser may return the product to the point of purchase for a full refund of the purchase price.

If the purchaser wishes to upgrade or convert to another CradlePoint, Inc. product within the thirty (30) day period, purchaser may return the product and apply the full purchase price toward the purchase of the other product. Any other return will be subject to CradlePoint, Inc.‘s existing return policy.

IN NO EVENT SHALL CRADLEPOINT‘S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS USER INTERFACE SOFTWARE, OR ITS DOCUMENTATION.

CradlePoint makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all user interface software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. CradlePoint reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity.

10.3 *Specifications*

MODEL NAME
MBR95 Wireless 4G/3G Router

WAN / INTERNET
3G/4G via USB modem; one default Ethernet port (10/100)

LAN
WiFi 802.11 b/g/n, four default Ethernet ports (10/100); one additional WAN Ethernet port re-configurable to LAN use

WIFI
2 internal 2.4 GHz WiFi antennas (600+ feet range)

Special Feature: Use WiFi as a Data Source. "WiFi-as-WAN" mode enables the MBR95 to become a WiFi repeater (using existing WiFi to create secure connections) or use as a WiFi-to-Ethernet adapter for non-WiFi devices.

Two WiFi Networks: 1 private SSID for owner, 1 public SSID for guests Create a private, secure, and prioritized connection while sharing with others. Each network can have its own QoS priorities and security settings.

BUTTONS / SWITCHES
WiFi On/Off Switch, WPS Button (WiFi Protected Setup), Modem Signal Strength, Reset, and Power Switch

LED INDICATORS
Power, Ethernet LAN (1-4), Ethernet WAN, 3G/4G WAN, 3G/4G Modem Status, WPS (WiFi Protected Setup), Signal Strength

DIMENSIONS
7.9-in x 5.3-in x 1.5-in (199.7mm x 134.7mm x 38.7mm), 0.5 lbs.

CERTIFICATIONS
FCC, IC, CE, WiFi Alliance, RoHS

TEMPERATURE
Operating: 0°C to 40 C / Storage: -4°F to 158°F

DETAILS

WAN Security NAT, SPI, ALG, inbound filtering of IP addresses, Port Blocking, Service Filtering (FTP, SMTP, HTTP, RPL, SNMP, DNS, ICMP, NNTP, POP3, SSH), Protocol filtering, WAN ping (allow/ignore)

Redundancy and Availability: Failover/Failback with 4G/3G/Cable/DSL or Satellite Modems

Intelligent Routing: UPnP, DMZ, Virtual Server/ Port Forwarding, Routing Rules, Route Management, Content Filtering, Website Filtering, Local DHCP server, DHCP Client, DNS DNS Proxy. ALGs: PPTP L2TP, PPPoE pass-through, IPSec pass-through, FTP (passive), FTP (active), MAC Address Filtering, Dynamic DNS Management Remote WAN Web-based

Management: Access (HTTP, HTTPS), Web-based Router Management Interface, One-button firmware upgrade, USB firmware upgrade, Modem Configuration and Management

Performance & Heath Monitoring: Traffic Shaping, WiPipe™ QoS, SSID-based priority, WAN port speed control, Modem Health Management (MHM) improves connectivity of 3rd-party USB modems.

VPN Pass-through support for laptop-based VPN clients

http://www.cradlepoint.com/